



**WESTELL**  
**VERSALINK™ GATEWAY (MODEL 327W)**

---

**USER GUIDE**



## TABLE OF CONTENTS

1. PRODUCT DESCRIPTION .....	4
2. SAFETY INSTRUCTIONS .....	4
3. REGULATORY INFORMATION .....	5
3.1 FCC Compliance Note.....	5
3.2 Canada Certification Notice.....	6
4. NETWORKING REQUIREMENTS .....	8
5. HARDWARE FEATURES.....	9
5.1 LED Indicators.....	9
5.2 Cable Connectors and Switch Locations .....	10
5.3 Connector Descriptions.....	10
5.4 Pinout Descriptions.....	11
6. INSTALLING THE HARDWARE.....	12
6.1 Installation Requirements .....	12
6.2 Before you begin.....	12
6.3 Microfilters .....	12
6.4 Hardware Installations .....	13
7. CONFIGURING VERSALINK FOR INTERNET CONNECTION .....	17
7.1 Setting Up an Account Profile .....	17
7.2 Confirm a DSL Sync .....	22
7.3 Establishing a PPP Session.....	24
7.4 Disconnecting a PPP Session.....	26
8. SETTING UP MACINTOSH OS X.....	28
9. SETTING UP ADVANCED CONFIGURATION .....	33
10. HOME .....	34
10.1 Adding Account Profiles .....	35
10.2 Editing Account Profiles.....	36
11. STATUS.....	38
11.1 Connection Summary .....	38
11.2 About .....	39
12. CONFIGURATION .....	40
12.1 Single Static IP – Single IP Address PassThrough .....	40
12.2 Service Configuration .....	45
12.3 Firewall Configuration.....	57
12.4 Wireless Configuration.....	62

12.5	Advanced LAN .....	68
12.6	Advanced WAN .....	84
13.	SETTING UP ADVANCED SERVICE CONFIGURATION .....	115
13.1	Port Forwarding Ranges of Ports .....	116
13.2	Adding Port Forwarding Ports .....	116
13.3	Port Forwarding Trigger Ports .....	117
13.4	Adding Local Trigger Ports .....	118
13.5	Static NAT .....	119
13.6	Enabling Static NAT .....	120
13.7	Disabling Static NAT .....	121
14.	MAINTENANCE .....	123
14.1	Backup/Restore .....	123
14.2	Firewall Log .....	124
14.3	Administrative Password .....	126
14.4	Remote Access .....	127
14.5	Update Device .....	128
15.	TROUBLESHOOTING .....	133
15.1	System Self Tests .....	133
15.2	Diagnostic Logs .....	135
15.3	Statistics .....	139
15.4	Wireless Statistics .....	142
15.5	Status .....	144
16.	NAT SERVICES .....	150
17.	HELP .....	154
18.	TECHNICAL SUPPORT INFORMATION .....	171
19.	WARRANTY AND REPAIRS .....	171
20.	PRODUCT SPECIFICATIONS .....	172
21.	SOFTWARE LICENSE AGREEMENT .....	173
22.	PUBLICATION INFORMATION .....	175

## 1. PRODUCT DESCRIPTION

The Westell® VersaLink™ Gateway provides reliable, high-speed, Internet access to your existing small office phone line. Your ADSL connection is “always-on” ending the hassles of dial-up modems and busy signals. Installation is easy ... no tools ... no headaches. Simply connect the hardware, apply power, and perform the simple software configuration for VersaLink and you are on the Internet.

VersaLink™ is capable of data rates hundreds of times faster than a traditional analog modem. But unlike analog modems, VersaLink™ allows you to use the same phone line for simultaneous voice/fax communications and high-speed Internet access, eliminating the need for dedicated phone lines for voice and data needs. VersaLink™ supports a variety of networking interfaces such as wireless 802.11b/g+, ADSL, Ethernet and the following optional features:

- VersaPort™: Alternate WAN uplink port
- Layer w/2 QOS with VLAN tagging
- HotSpot
- Simultaneous public/private network support

Hereafter, the Versa Link™ Gateway will be referred to as “Gateway” or “Modem.”

## 2. SAFETY INSTRUCTIONS

Never install any telephone wiring during a lightning storm.

Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.

Never touch non-insulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.

Use caution when installing or modifying telephone lines.



### **WARNING**



**Risk of electric shock. Voltages up to 140 Vdc (with reference to ground) may be present on telecommunications circuits.**

## **3. REGULATORY INFORMATION**

### **3.1 FCC Compliance Note**

(FCC ID: CH8-327WXX-6)

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the Federal Communication Commission (FCC) Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy, and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment OFF and ON, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment to a different circuit from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

**Modifications made to the product, unless expressly approved by Westell Inc., could void the users' right to operate the equipment.**

#### **RF EXPOSURE**

**This device has been tested and complies with FCC RF Exposure (SAR) limits in typical laptop computer configurations and this device can be used in desktop or laptop computers with side-mounted PCMCIA slots, which can provide 1 cm separation distance from the antenna to the body of the user or a nearby person. Thin laptop computers may need special attention to maintain antenna spacing while operating. This device cannot be used with handheld PDAs (personal digital assistants). Use in other configurations may not ensure compliance with FCC RF exposure guidelines. This device and its antenna must not be co-located or operate in conjunction with another antenna or transmitter.**

#### **PART 68 - COMPLIANCE REGISTRATION**

This equipment (Model 327W) complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. A label on the bottom of this equipment contains, among other information, the Ringer Equivalence Number (REN) and the product identifier. For products approved after July 23, 2001 the product identifier is in the format US:AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point (e.g. 03 is a REN of 0.3). The REN is used to determine the number of devices that may be connected to a telephone line. For earlier products, the REN is separately shown on the label. If requested, this number must be provided to the telephone company.

Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company.

This equipment is designated to connect to the telephone network or premises wiring using a compatible modular jack that is Part 68 compliant. An FCC compliant telephone cord and modular plug is provided with the equipment. See the Installation Information section of this User Guide for details.



A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instruction for details.

If this terminal equipment (Model 327W) causes harm to the telephone network, the telephone company may request you to disconnect the equipment until the problem is resolved. The telephone company will notify you in advance if temporary discontinuance of service is required. If advance notification is not practical, the telephone company will notify you as soon as possible. You will be advised of your right to file a complaint with the FCC if you believe such action is necessary.

If you experience trouble with this equipment (Model 327W), do not try to repair the equipment yourself. The equipment cannot be repaired in the field. Contact your ISP, or contact the original provider of your DSL equipment.

The telephone company may make changes to their facilities, equipment, operations, or procedures that could affect the operation of this equipment. If this happens, the telephone company will provide advance notice in order for you to make the modifications necessary to maintain uninterrupted service.

If your home has specially wired alarm equipment connected to the telephone line, ensure that the installation of this equipment (Model 327W) does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

This equipment cannot be used on public coin phone service provided by the telephone company. Connection of this equipment to party line service is subject to state tariffs.

## 3.2 Canada Certification Notice

The Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operations and safety requirements as prescribed in the appropriate Terminal Equipment Technical Requirements document(s). The department does not guarantee the equipment will operate to the user's satisfaction.

This equipment meets the applicable Industry Canada Terminal Equipment Technical Specification. This is confirmed by the registration number. The abbreviation, IC, before the registration number signifies that registration was performed based on a Declaration of Conformity indicating that Industry Canada technical specification were met. It does not imply that Industry Canada approved the equipment. The Ringer Equivalence Number (REN) is 0.0. The Ringer Equivalence Number that is assigned to each piece of terminal equipment provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local Telecommunication Company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations. Connection to a party line service is subject to state tariffs. Contact the state public utility commission, public service commission, or corporation commission for information.

If your home has specially wired alarm equipment connected to the telephone line, ensure that the installation of this equipment (Model 327W) does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

If you experience trouble with this equipment (Model 327W), do not try to repair the equipment yourself. The equipment cannot be repaired in the field and must be returned to the manufacturer. Repairs to certified equipment

should be coordinated by a representative, and designated by the supplier. Refer to section 19 in this User Guide for further details.

The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed five.

Users should ensure, for their own protection, that the electrical ground connections of the power utility, telephone lines, and internal, metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

**CAUTION**

**Users should not attempt to make such connections themselves, but should contact the appropriate electrical inspection authority, or electrician, as appropriate.**

## 4. NETWORKING REQUIREMENTS

The following system specifications are required for optimum performance of the VersaLink™ via 10/100 Base-T or Wireless installations.

CONNECTION TYPE	MINIMUM SYSTEM REQUIREMENTS	NETWORKING SCHEME
ETHERNET	<ul style="list-style-type: none"><li>• Pentium® or equivalent class machines</li><li>• Microsoft® Windows® (95, 98, ME, NT 4.0, 2000, or XP) Macintosh® OS X, or Linux installed</li><li>• 64 MB RAM (128 MB recommended)</li><li>• 10 MB of free hard drive space</li><li>• TCP/IP Protocol stack installed</li><li>• 10/100 Base-T Network Interface Card (NIC)</li><li>• Computer Operating System CD-ROM on hand</li></ul>	Networking via 10/100 Base-T Ethernet requires an available Ethernet port with a 10/100 Base-T Network Interface Card (NIC) installed.
WIRELESS IEEE 802.11g	<ul style="list-style-type: none"><li>• Pentium® or equivalent class machines</li><li>• Microsoft® Windows® (98, ME, 2000, or XP) or Macintosh® OS X installed</li><li>• Computer Operating System CD-ROM on hand</li><li>• Internet Explorer 4.x or Netscape Navigator 4.x or higher</li><li>• 64 MB RAM (128 MB recommended)</li><li>• 10 MB of free hard drive space</li><li>• An available IEEE 802.11b/g/g+ PC adapter</li></ul>	Networking via Wireless or other 802.11b/g/g+ capable network adapter card.

## 5. HARDWARE FEATURES

### 5.1 LED Indicators

This section explains the LED States and Descriptions. LED indicators are used to verify the unit's operation and status.

**LED States and Descriptions**

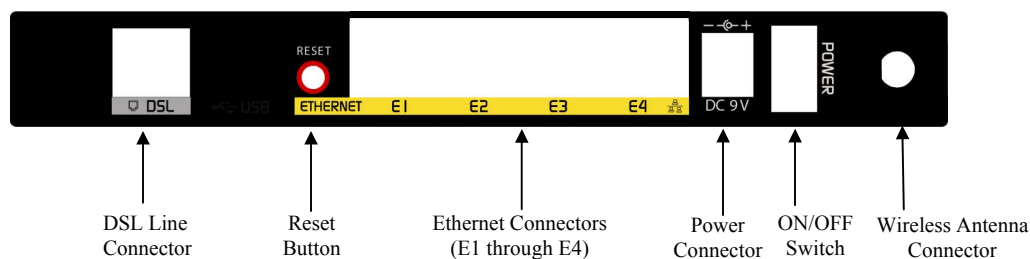
LED	State	Description
<b>POWER</b>	<b>Solid Green</b>	Modem power is ON.
	<b>OFF</b>	Modem power is OFF.
	<b>Solid Red</b>	POST (Power On Self Test), Failure (not bootable) or Device Malfunction. Note: The Power LED should be red no longer than two seconds after the power on self test passes.
<b>ETHERNET</b> (E1, E2, E3, E4)	<b>Solid Green</b>	Powered device is connected to the associated port (includes devices with wake-on LAN capability where slight voltage is supplied to an Ethernet connection). Note: When using the optional uplink port (E1), Ethernet LAN connection is limited to E2, E3, and E4.
	<b>Flashing Green</b>	10/100 Base-T LAN activity is present (traffic in either direction)
	<b>OFF</b>	Modem power is OFF, no cable or no powered device is connected to the associated port.
<b>WIRELESS</b>	<b>Solid Green</b>	Link Established.
	<b>Flashing Green</b>	Wireless LAN activity is present (traffic in either direction).
	<b>OFF</b>	Modem power is OFF or No Link.
<b>DSL</b>	<b>Solid Green</b>	Good DSL sync.
	<b>Flashing Green</b>	DSL attempting to sync.
	<b>OFF</b>	Modem power is OFF.
<b>INTERNET</b>	<b>Solid Green</b>	Internet link established.
	<b>Flashing Green</b>	IP connection established and IP Traffic is passing through device (in either direction). Note: If the IP or PPP session is dropped due to an idle timeout, the light will remain solid green, if an ADSL connection is still present. If the session is dropped for any other reason, the light is turned OFF. The light will turn red when it attempts to reconnect and DHCP or PPP fails).
	<b>Solid Red</b>	Device attempted to become IP connected and failed (no DHCP response, no PPP response, PPP authentication failed, no IP address from IPCP, etc.).
	<b>OFF</b>	Modem power is OFF, Modem is in Bridge Mode, or the connection is not present.

*NOTE: Safe Boot is reflected when the Power and Internet LED's are both Red and all other LED's are off.*

## 5.2 Cable Connectors and Switch Locations



- DSL connector (RJ-11)
- Reset button
- (4) Ethernet connector (RJ-45) with optional uplink port  
(Note: When using the optional uplink port (E1), Ethernet LAN connection is limited to E2, E3, and E4.
- Power connector (barrel)
- Wireless IEEE 802.11b/g SMA connector and antenna

Note: When using the optional uplink port (E1), Ethernet LAN connection is limited to E2, E3, and E4. The UPLINK feature is optional, and if UPLINK is not enabled in the .ini file, the Gateway will use DSL and Wireless only.



## 5.3 Connector Descriptions

The following chart displays the connector types.

SYMBOL	NAME	TYPE	FUNCTION
	DSL LINE	6-pin RJ-11 modular jack	Connects to an ADSL-equipped telephone jack or DSL connection of a POTS splitter.
<b>DC 9V</b>	POWER	Barrel connector	Power source.
	ETHERNET	8-pin (RJ-45) modular jack	Connects the Ethernet device to the PC.
<b>Wireless</b>	ANTENNA	SMA connector and antenna	Connects to wireless IEEE 802.11b/g/g+

## 5.4 Pinout Descriptions

The following tables list the pinout descriptions.

**DSL Pinouts**

<b>Pinout</b>	<b>Description</b>
1, 2, 5, 6	Not Used
3	DSL Tip
4	DSL Ring

**Ethernet/Optional Uplink Port Pinouts**

<b>Pinout</b>	<b>Description</b>
1	Rx+
2	Rx-
3	Tx+
4,5,7,8	Not Used
6	Tx-

## **6. INSTALLING THE HARDWARE**

### **6.1 Installation Requirements**

To install VersaLink™, you will need the following:

- A Network Interface Card (NIC) installed in your PC, or
- An IEEE 802.11b/g adapter

NOTE: Internet service provider subscriber software and connection requirements may vary. Consult your ISP for installation instructions. Please wait until you have received notification from your ISP that your DSL line has been activated before installing VersaLink™ and the software.

### **6.2 Before you begin**

Make sure that your kit contains the following items:

- Westell VersaLink™ Gateway
- Power Supply
- RJ-45 Ethernet cable
- RJ-11 Phone cable
- SMA Antenna
- Westell CD-ROM containing User Guide in PDF format
- Quick Start Guide

### **6.3 Microfilters**

ADSL signals must be blocked from reaching each telephone, answering machine, fax machine, computer modem or any similar conventional device. Failure to do so may degrade telephone voice quality and ADSL performance. Install a microfilter if you desire to use the DSL-equipped line jack for telephone, answering machine, fax machine or other telephone device connections. Microfilter installation requires no tools or telephone rewiring. Just unplug the telephone device from the baseboard or wall mount and snap in a microfilter, next snap in the telephone device. You can purchase microfilters from your local electronics retailer, or contact the original provider of your DSL equipment.

## 6.4 Hardware Installations





**NOTE:** Please wait until you have received notification from your ISP that your DSL line has been activated before installing VersaLink.

**NOTE:** If you are using VersaLink™ in conjunction with an Ethernet Hub or Switch, refer to the manufacturer's instructions for proper installation and configuration. When using a Microfilter, be certain that the DSL phone cable is connected to the "DSL/HPN" non-filtered jack. **Westell recommends the use of a surge suppressor to protect equipment attached to the power supply.**

### 6.4.1 Installation via 10/100 Base-T Ethernet



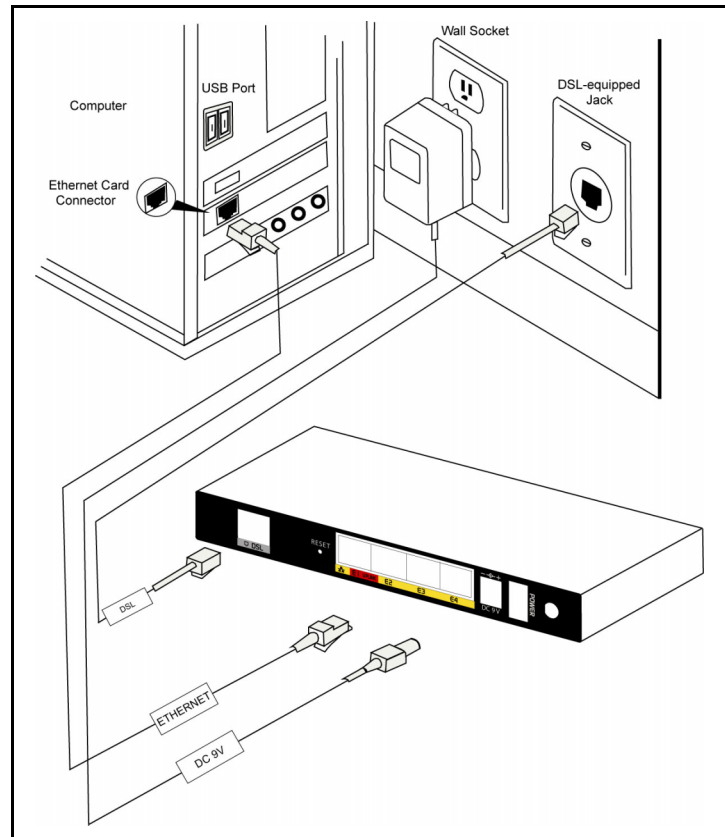
**NOTE:** Before you connect via 10/100 Base-T, you must have an available Ethernet card installed in your computer. If your Ethernet card does not auto-negotiate, you must set it to half duplex. Refer to the Ethernet card manufacturer's instructions for installing and configuring your Ethernet card.

1. Connect the power supply cord to the power connector marked **DC 9V** on the rear panel of VersaLink. Plug the other end of the power supply into a wall socket.
2. Connect the DSL phone cable from the jack marked  on the rear panel of VersaLink to the DSL-equipped telephone line jack on the wall. **IMPORTANT:** Do not use a DSL filter on this connection. You must use the phone cord that was provided with the kit.
3. Connect the yellow Ethernet cable from any one of the Ethernet jacks marked  on the rear panel of VersaLink to the Ethernet port on your computer. **Repeat this step to connect up to three additional PCs to VersaLink.**

**NOTE:** You may connect to any of the four Ethernet jacks on the rear panel as they serve as an Ethernet switch. However, when using the optional uplink port (E1), Ethernet LAN connection is limited to ports E2, E3, and E4.

4. Check to see if the DSL LED is solid green. If the DSL LED is solid green, VersaLink is functioning properly.
5. Check to see if the Ethernet LED is solid green. Solid green indicates that the Ethernet connection is functioning properly.

Congratulations! You have completed the Ethernet hardware installation. No software installation is required when using only an Ethernet connection. Proceed to section 7 to configure VersaLink for Internet connection.




**Figure 1. Connection via 10/100 Base-T Ethernet**

## 6.4.2 Connecting PCs via Wireless

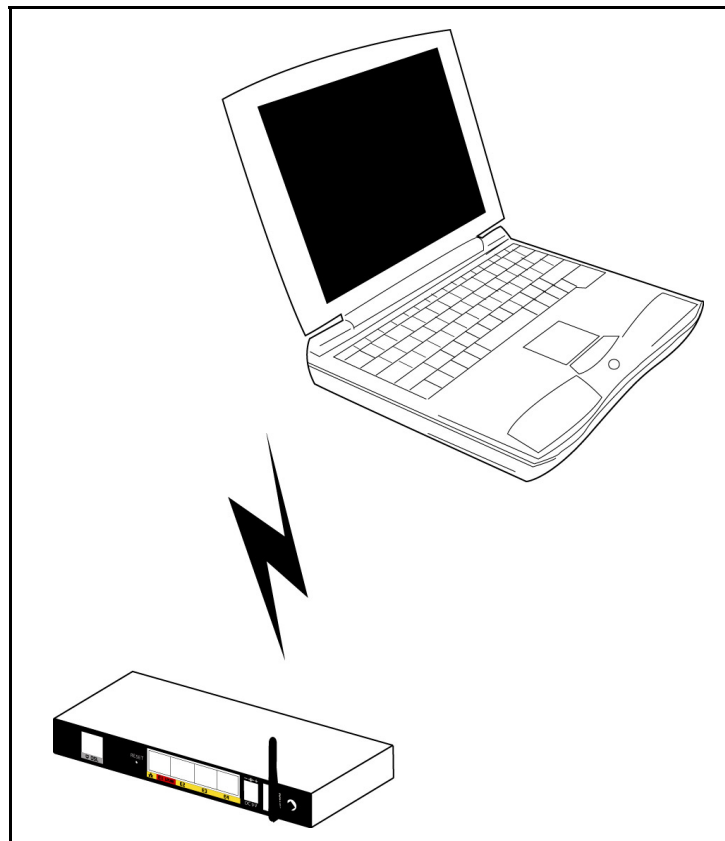
**IMPORTANT:** If you are connecting to VersaLink via a wireless network adapter, the SSID must be the same for both VersaLink and your PC's wireless network adapter. The default SSID for VersaLink is the serial number of the unit (located below the bar code on the bottom of the unit and also on the Westell shipping carton). Locate and run the utility software provided with your PC's Wireless network adapter and enter the SSID value. The PC's wireless network adapter must be configured with the SSID (in order to communicate with VersaLink) before you begin the account setup and configuration procedures. Later, for privacy you can change the SSID by following the procedures outlined in section 12.4 (Wireless Configuration).

**NOTE:** Client PCs can use any Wireless Fidelity (Wi-Fi) 802.11b/g certified card to communicate with VersaLink. The Wireless card and VersaLink must use the same Wired Equivalent Privacy (WEP) security code type. The factory default for WEP is DISABLED. If you enable WEP, you must ensure the network setting for your wireless adapter is set to "Must Use Shared Key for WEP" or "Open Wi-Fi." You must ensure that your PC's Wi-Fi adapter is configured properly for whichever network setting you use. You can access the settings in the advanced properties of the wireless network adapter.

To network VersaLink to additional computers in your home or office using a wireless installation, you will need to confirm the following:

1. Ensure that an 802.11b/g/g+ wireless network adapter has been installed in each PC on your wireless network.
2. Install the appropriate drivers for your Wireless IEEE802.11b or IEEE802.11g adapter.
3. Make sure the SMA antenna connector is loose. Orient the antenna in the proper configuration. Then, tighten the antenna knob to lock it into place.
4. Connect the power supply cord to the power connector marked **DC 9V** on the rear panel of VersaLink. Plug the other end of the power supply into a wall socket.
5. Connect the DSL phone cable from the connector marked  on the rear panel of VersaLink to the DSL-equipped telephone line jack on the wall. **IMPORTANT:** Do not use a DSL filter on this connection. You must use the phone cord that was provided with the VersaLink kit.
6. Check to see if the DSL LED is solid Green. If the DSL LED is solid Green, VersaLink is functioning properly.
7. Check to see if VersaLink's Wireless LED is solid Green. This means that the Wireless interface is functioning properly.

Congratulations! You have completed the Wireless installation VersaLink. You must now go to section 7 to configure VersaLink for Internet connection.





**Figure 2. Connection via Wireless**

### 6.4.3 Ethernet and Wireless Combination Installation

The VersaLink™ supports simultaneous use of 10/100 Base-T Ethernet and Wireless configurations. The following instructions explain how to install VersaLink for simultaneous use of Ethernet and Wireless ports.

NOTE: Refer to Figure 1 and Figure 2 for instructions on hardware installation via Ethernet and Wireless connections.

1. Ensure that an 802.11b/g+ wireless network adapter has been installed in each PC on your wireless network
2. Install the appropriate drivers for your Wireless IEEE802.11b or IEEE802.11g adapter.
3. Make sure the SMA antenna connector is loose. Orient the antenna in the proper configuration. Then, tighten the antenna knob to lock it into place.
4. Connect the power supply cord to the power connector marked **DC 9V** on the rear panel of VersaLink. Plug the other end of the power supply into a wall socket.
5. Connect the DSL phone cable from connector marked  on the rear panel of VersaLink to the DSL-equipped telephone line jack on the wall. **IMPORTANT: Do not** use a DSL filter on this connection. You must use the phone cord that was provided with the kit.
6. Connect the yellow Ethernet cable from any one of the Ethernet jacks marked  on the rear panel of VersaLink to the Ethernet port on your computer. **Repeat this step to connect up to three additional PCs to VersaLink.**

NOTE: You may connect to any of the four Ethernet jacks on the rear panel as they serve as an Ethernet switch. However, when using the optional uplink port (E1), Ethernet LAN connection is limited to ports E2, E3, and E4.

7. Check to see if the DSL LED is solid green. If the DSL LED is solid green, VersaLink is functioning properly.
8. Check to see if the Ethernet LED is solid green. Solid green indicates that the Ethernet connection is functioning properly.
9. Check to see if VersaLink's Wireless LED is solid green. This means that the Wireless interface is functioning properly.

Congratulations! You have completed the simultaneous hardware (Ethernet and Wireless) installation. You must now go to section 7 to configure VersaLink for Internet connection.

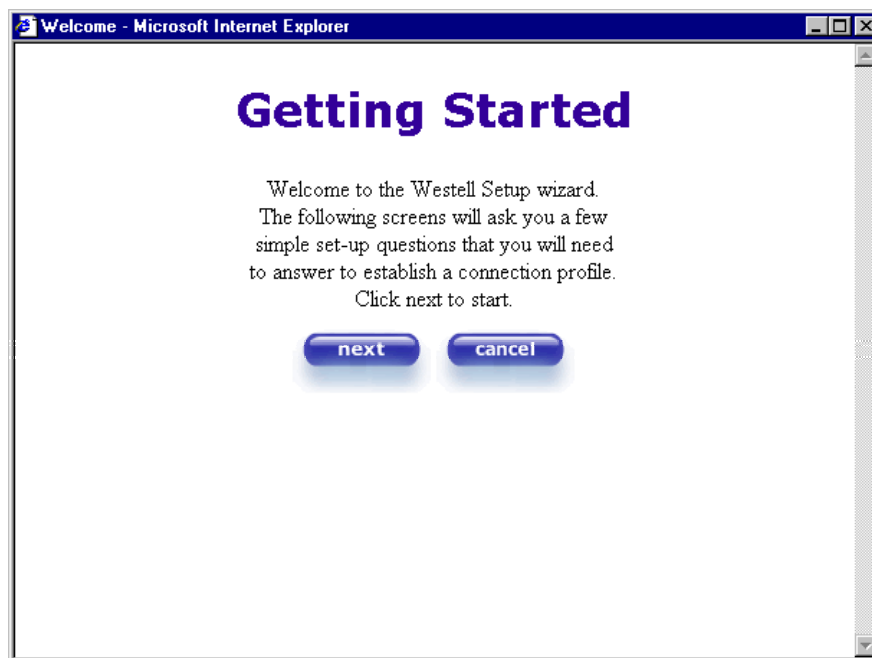
## 7. CONFIGURING VERSALINK FOR INTERNET CONNECTION

To browse the Internet using VersaLinK™, you must set up your account profile, confirm your DSL sync, and establish a PPP session with your Internet Service Provider (ISP). Refer to the Internet service provider's installation manual to install the software required for your Internet connection.

NOTE: Internet service provider subscriber software and connection requirements may vary. Consult your Internet service provider for installation instructions.

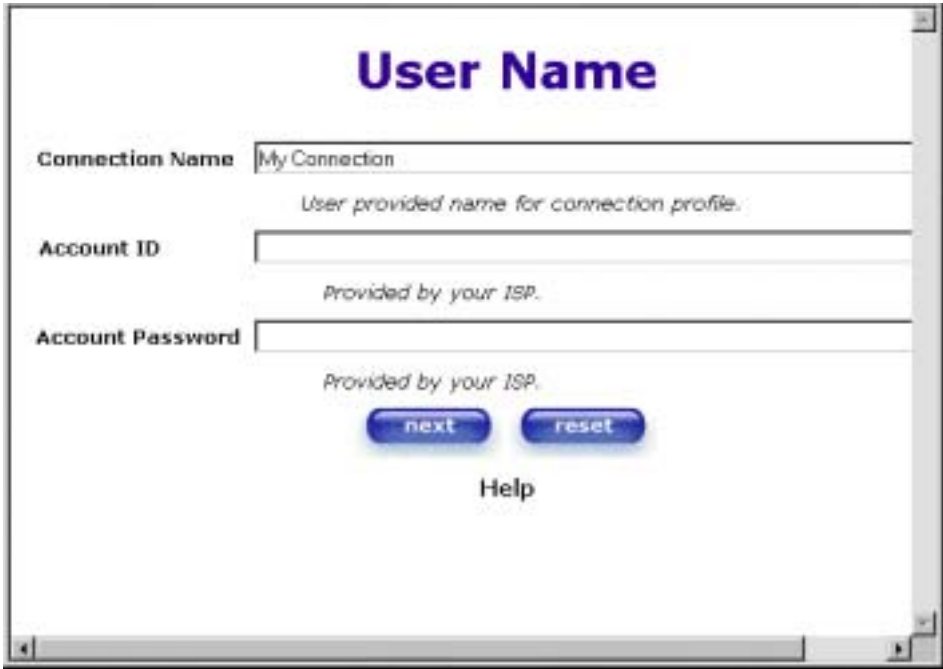
### 7.1 Setting Up an Account Profile

After connecting VersaLink, bring up your Web browser and type either **http://dslrouter** or **http://192.168.1.1** in the browser's address window and press 'Enter' on your keyboard. The **Getting Started** screen will appear. Click on **next**.



If you clicked on **Next**, the following screen will be displayed. This screen will allow you to set up your account profile.

**NOTE:** Before you set up your account profile, you must obtain your **Account ID**, **Account Password**, and **VPI/VCI** values from your Internet service provider. You will use this information when you set up your account parameters. If you are at a screen and need help, click on the **Help** button to learn more about the screen, or see section 17 (Help) for additional information on the help messages.

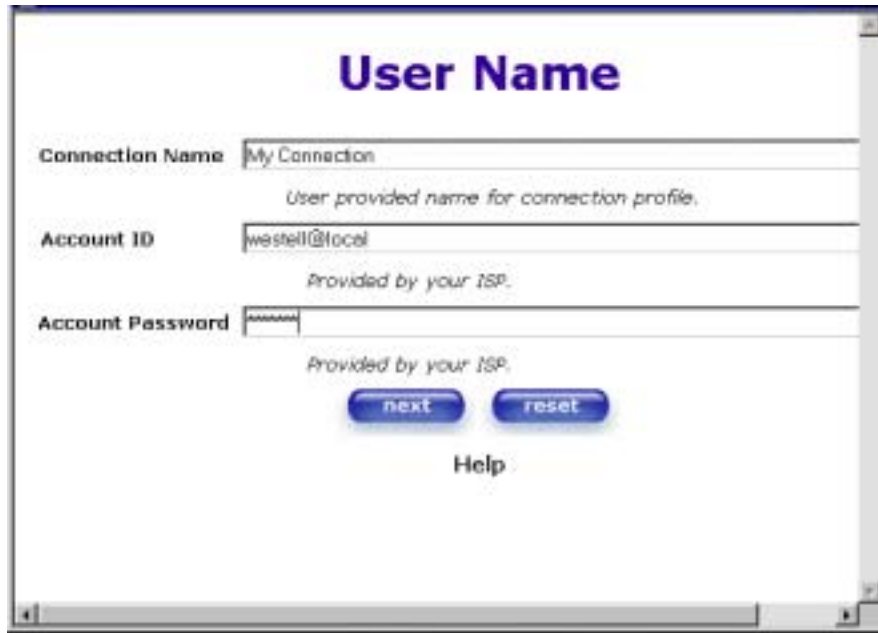


The image shows a web browser window titled "User Name". It contains three input fields: "Connection Name" with the text "My Connection" and a hint "User provided name for connection profile."; "Account ID" with a hint "Provided by your ISP."; and "Account Password" with a hint "Provided by your ISP.". Below the fields are two buttons labeled "next" and "reset", and a link labeled "Help".

Type in your account parameters. (Account parameters are required before connecting to the Internet.)  
Account Parameters include:

- **Connection Name**-the Connection Name is a word or phrase that you use to identify your account.  
(You may enter up 64 characters in this field.)
- **Account ID**-the Account ID is provided by your Internet Service Provider.  
(You may enter up 255 characters in this field.)
- **Account Password**-the Account Password is provided by your Internet Service Provider.  
(You may enter up 255 characters in this field.)

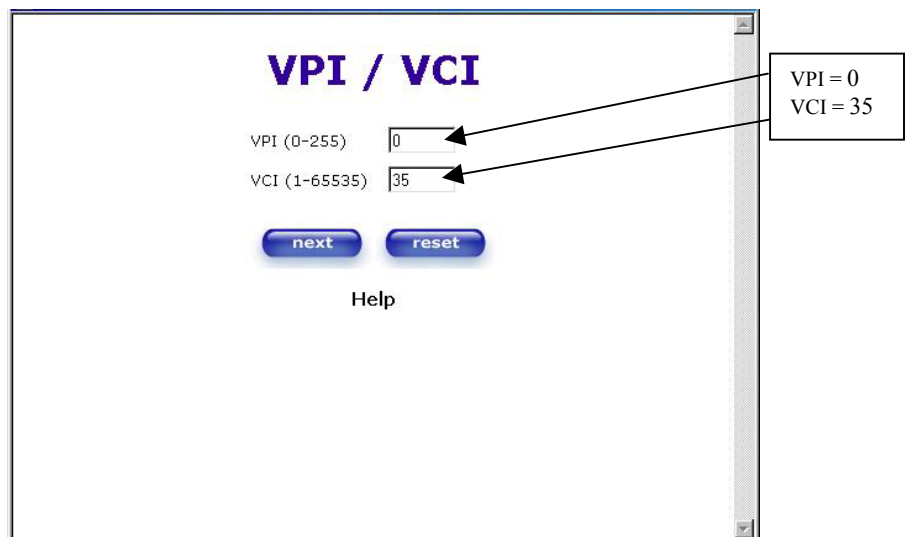
When you enter your account parameters at the **User Name** screen, they will be displayed as shown in the screen below. Click **next** if you want your account parameters to take effect. Click on **reset** if you do not want the account parameters that you entered to take effect or if you want to re-enter the parameters.



The 'User Name' configuration screen displays three input fields: 'Connection Name' with the value 'My Connection', 'Account ID' with the value 'westell@local', and 'Account Password' which is masked with asterisks. Below each field is a descriptive note: 'User provided name for connection profile.', 'Provided by your ISP.', and 'Provided by your ISP.' respectively. At the bottom, there are 'next' and 'reset' buttons, and a 'Help' link.

Enter the VPI and VCI values (**0** for VPI and **35** for VCI default) you obtained from your Internet service provider. The actual VPI/VCI values may vary according to your ISP. Click on **next**.

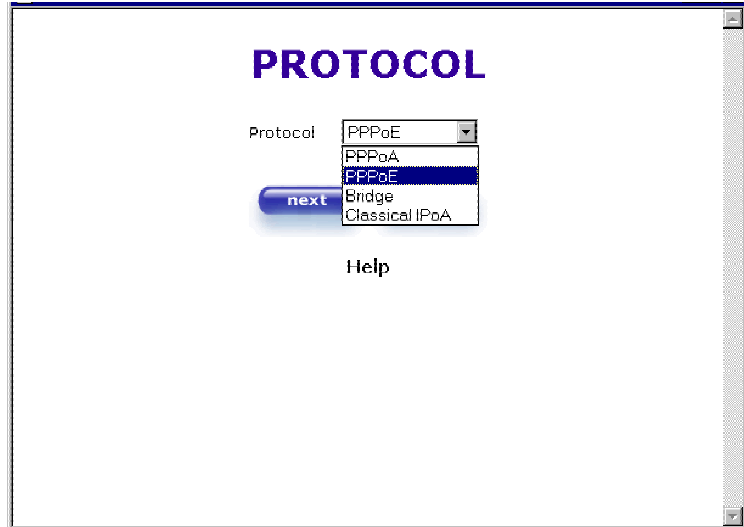
NOTE: Depending on your Internet Service Provider, the **VPI/VCI** screen may come pre-configured and it will be displayed here. In this case, you should not change any values in this screen. Click on **next** to go to the **PROTOCOL** screen.



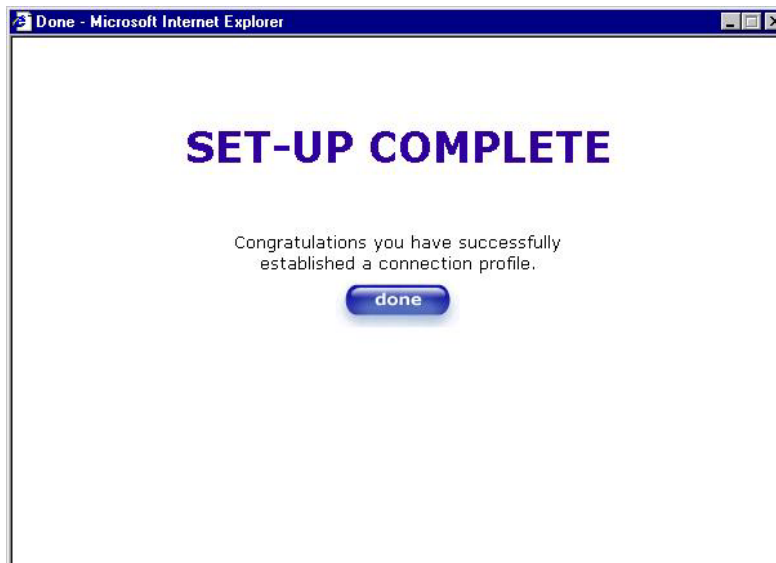
The 'VPI / VCI' configuration screen shows two input fields: 'VPI (0-255)' with the value '0' and 'VCI (1-65535)' with the value '35'. Arrows from a callout box on the right point to these values. The callout box contains the text 'VPI = 0' and 'VCI = 35'. Below the fields are 'next' and 'reset' buttons, and a 'Help' link.

Select the Protocol type that you obtained from your Internet service provider. Click on **next**.

NOTE: Depending on your Internet Service Provider, the **PROTOCOL** screen may come pre-configured and it will be displayed here. In this case, you will need to click on **next** to go to the **SET-UP COMPLETE** screen.

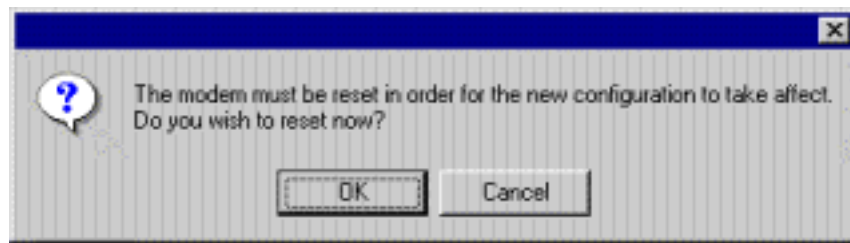


When the **SET-UP COMPLETE** screen appears, you have successfully completed your Account Profile setup. Click on **done**.



If you changed the **VPI/VCI** settings and clicked on **done** in the **SET-UP COMPLETE** screen, the following screen will appear. Click on **OK**.

NOTE: The following pop-up will appear only if you have changed the **VPI**, **VCI**, or **Protocol** values in the preceding screens. If you did not change any of these values, this pop-up screen will not appear and the Gateway will not be reset. If your Gateway's connection setting is set to "Always On" and you have changes any of these values, the Gateway will reset automatically. For instructions on editing your connection settings, see section 10.2.



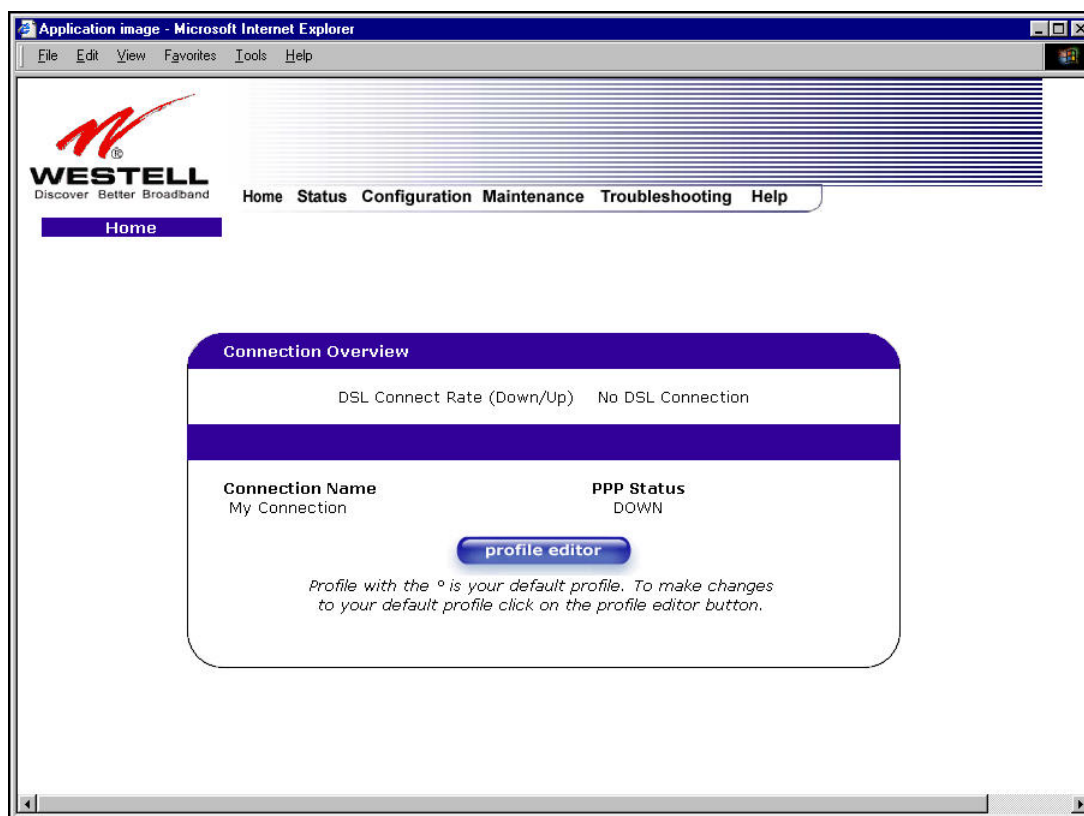
If you clicked on **OK**, the following screen will be displayed. VersaLink™ will be reset and the new configuration will take effect. Next, proceed to section 7.2 to confirm your DSL sync.



## 7.2 Confirm a DSL Sync

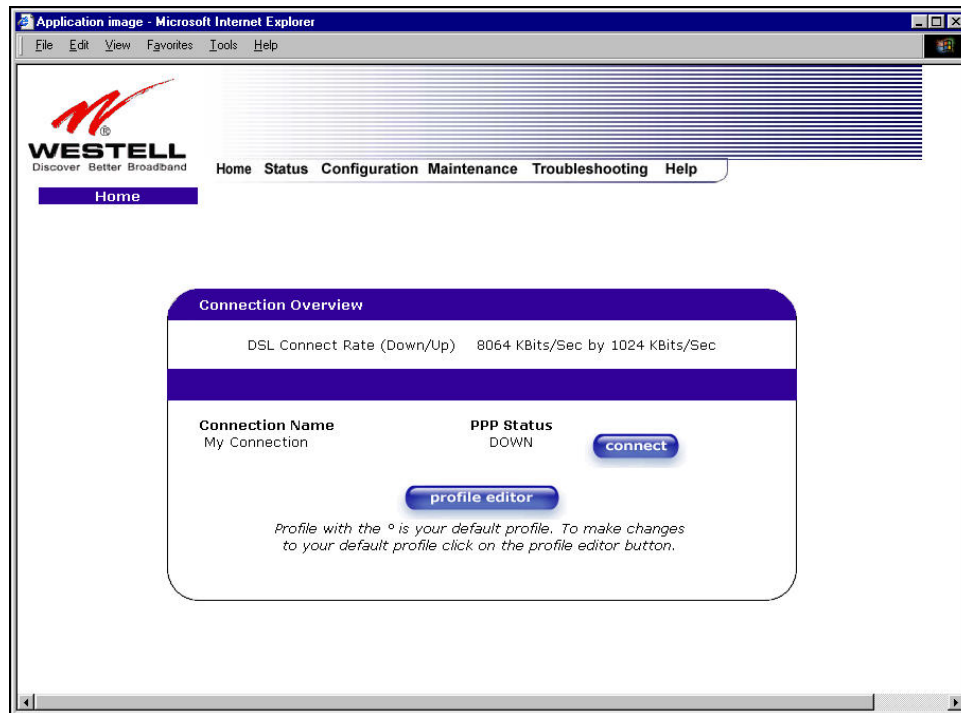
Remember, you must have active DSL service before VersaLink can synchronize with your ISP's equipment. To determine if VersaLink has a DSL sync, view the DSL Connection Rate in the **Connection Overview** section (see the following Home page). If the status reads **No DSL Connection**, check the DSL physical connection, explained in section 6 (INSTALLING THE HARDWARE) of this User Guide.

NOTE: If no DSL sync is established, the **connection** button will not be displayed in the following screen. To determine if the DSL sync is established, check VersaLink's DSL/RDY LED. If the DSL/RDY LED is not solid green, you do not have a DSL sync established. Contact your ISP for further instructions.



The following screen shows the DSL connection rate with values that indicate a successful DSL SYNC has been established. The connection rate values represent the transmission speed of your DSL line. (The Gateway may take time to report these values.) Click on the **Connect** button to establish a PPP session.

NOTE: VersaLink will handle transmission rates up to 8 Mbps. Your actual DSL rates may vary depending on your Internet service provider.

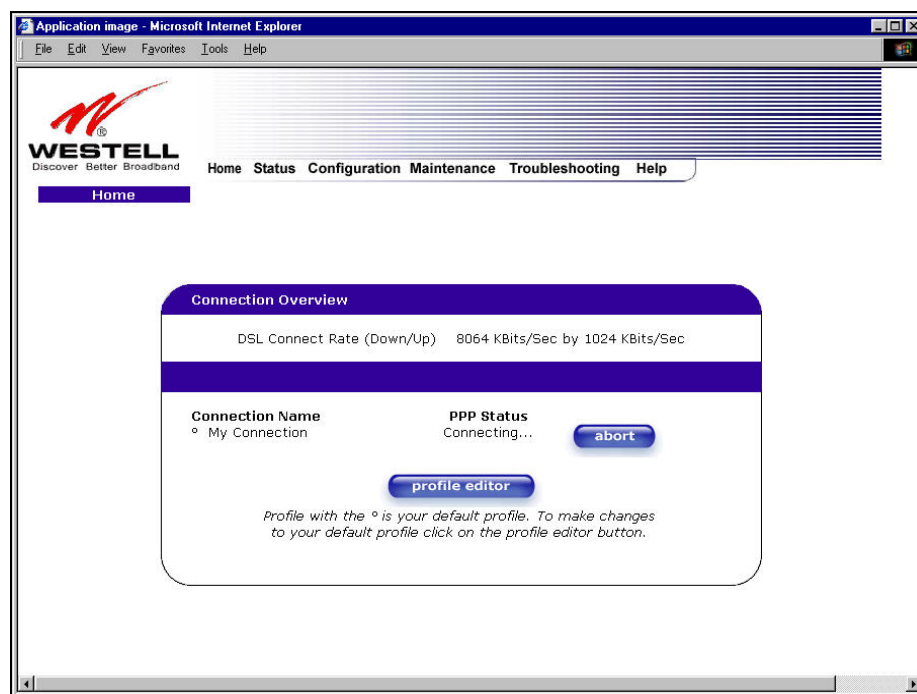


## 7.3 Establishing a PPP Session

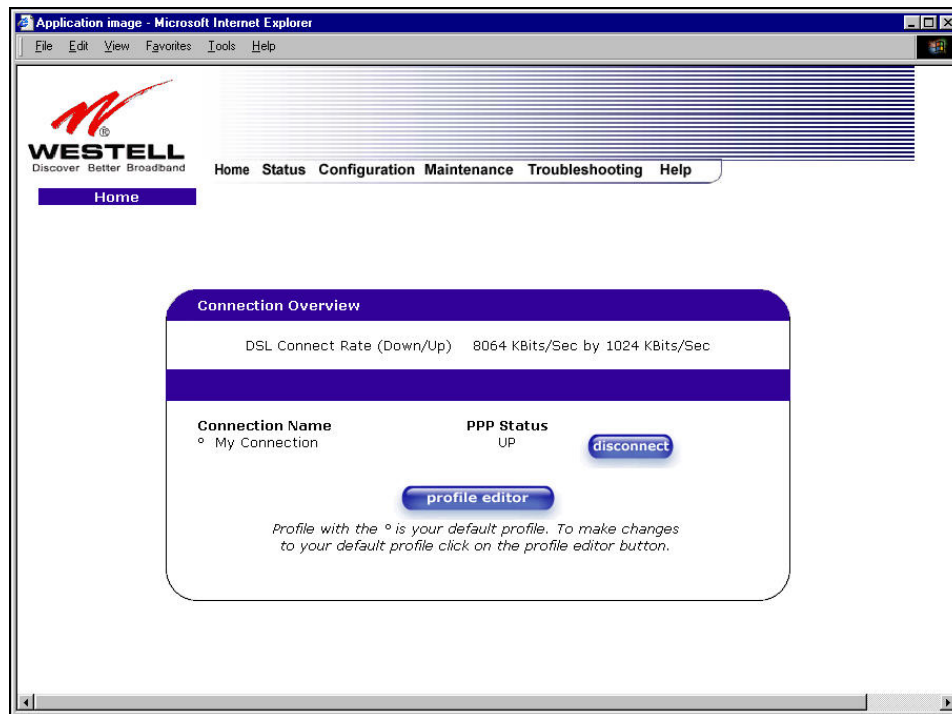
View the **PPP Status** at the Home page. If the PPP Status displays **DOWN**, click the **Connect** button to establish a PPP session.

NOTE: Whenever the PPP Status displays **DOWN**, you do not have a PPP session established. If your Gateway's connection setting is set to "Always On" or "On Demand," after a brief delay the PPP session will be established automatically and the PPP Status will display **UP**. If the connection setting is set to "Manual," you must click on the **Connect** button to establish a PPP session. Once the PPP session has been established (PPP Status displays **UP**), you may proceed with your Gateway's configuration. Section 10.2 provides instructions on editing the connection settings. (Refer to the 'Edit My Connection' screen.) VersaLink's factory default connection setting is "Manual."

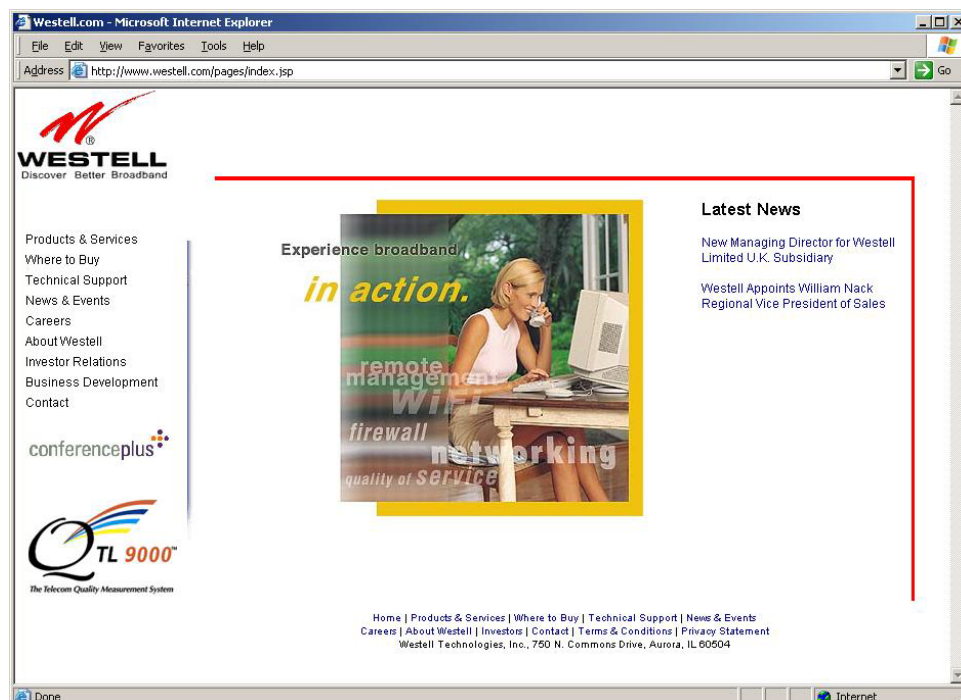
If you click the **Connect** button, the following screen will appear briefly. The **PPP Status** in the **Connection Overview** window allows you to view the state of your ISP connection. When the **PPP Status** displays **Connecting...**, this means that you are establishing a PPP session.



After a PPP session has been established, the **PPP Status** will display **UP**. Congratulations! You may now browse the Internet.



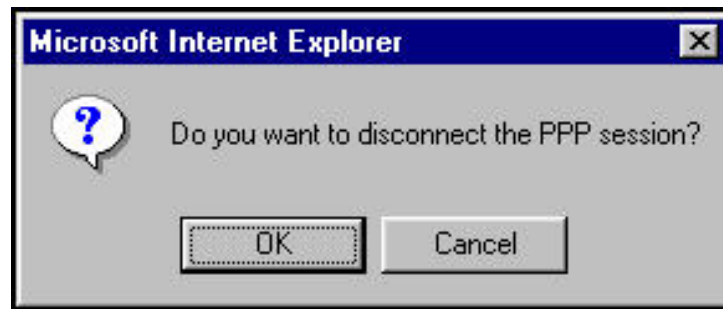
For example, if you want to visit Westell's home page, type **http://www.westell.com** in your browser's address window.



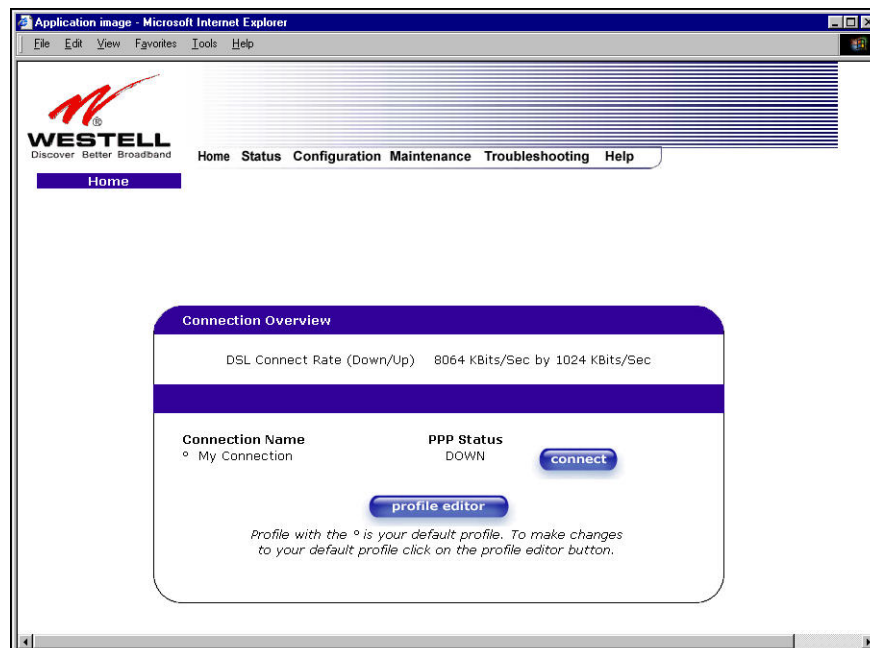
## 7.4 Disconnecting a PPP Session

If you have finished browsing the Internet and want to disconnect from your Internet service provider, click on the **Disconnect** button in the **Connection Overview** screen (the preceding screen). The following pop-up screen will appear. Click on **OK** to disconnect the PPP session.

Warning: If you disconnect the PPP session, this will disconnect the Gateway from the Internet, and all users will be disconnected until the PPP session is re-established.



If you clicked the **Disconnect** button in the preceding **Connection Overview** screen, the **PPP Status** should display **DOWN**. This means that you no longer have a PPP session (no IP connection to your Internet service provider). However, your DSL session will not be affected. When you are ready to end your DSL session, simply power down VersaLink via the power switch on VersaLink's rear panel.



When you are ready to establish a PPP session, click on the **connect** button. (If you powered down VersaLink, you must first power up VersaLink and log on to your account profile before you establish a PPP session.)

NOTE: When you are ready to exit VersaLink's interface, click on the **X** (close) in the upper-right corner of the window. Closing the window will not affect your PPP Status (your PPP session will not be disconnected). You must click on the **disconnect** button to disconnect your PPP session. When you are ready to restore this interface, you



must launch your Internet browser and type **http://dslrouter/** or type **http://192.168.1.1/** in the browser's address window and press 'Enter' on your keyboard.

## 8. SETTING UP MACINTOSH OS X

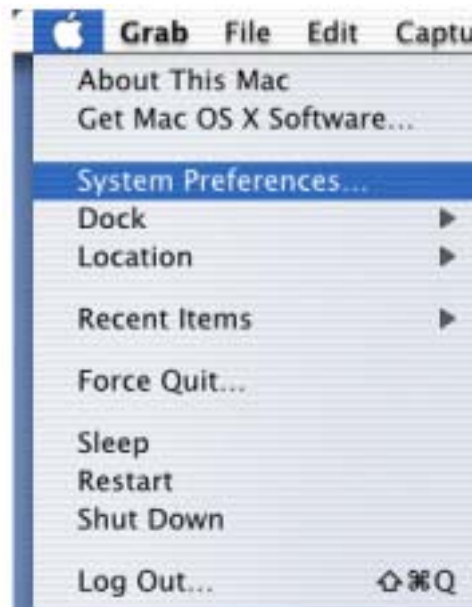
This section provides instructions on how to use Macintosh Operating System 10 with VersaLink. Follow the instructions in this section to create a new network configuration for Macintosh OS X.



NOTE: Macintosh computers must use VersaLink's Ethernet installation. Refer to section 6, (INSTALLING THE HARDWARE).

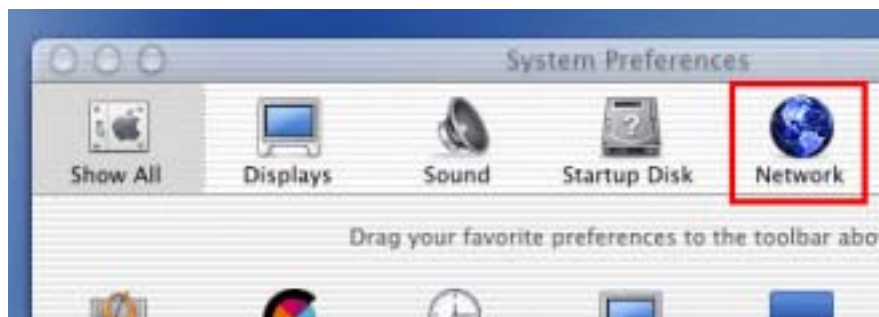
### Open the System Preference Screen

After you have connected the Westell VersaLink to the Ethernet port of your Macintosh, the screen below will appear. Click on the “**Apple**” icon in the upper-right corner of the screen and select **System Preferences**.



### Choose the Network Preferences

After selecting **System Preferences...**, from the previous screen, the **System Preferences** screen will be displayed. From the **System Preferences** screen, click on the **Network** icon.



## Create a New Location

After selecting the **Network** icon at the **System Preferences** screen, the **Network** screen will be displayed. Select **New Location** from the **Location** field.



## Name the New Location

After selecting **New Location** from the **Network** screen, the following screen will be displayed. In the field labeled **Name your new location:**, change the text from “Untitled” to “Westell.” Click **OK**.



## Select the Ethernet Configuration

After clicking on **OK** in the preceding screen, the **Network** screen will be displayed. The **Network** screen shows the settings for the newly created location. From the **Configure** field in the **Network** screen, select **Built-in Ethernet**. Click on **Save**.

**NOTE:** Default settings for the Built-in Ethernet configuration are sufficient to operate VersaLink.

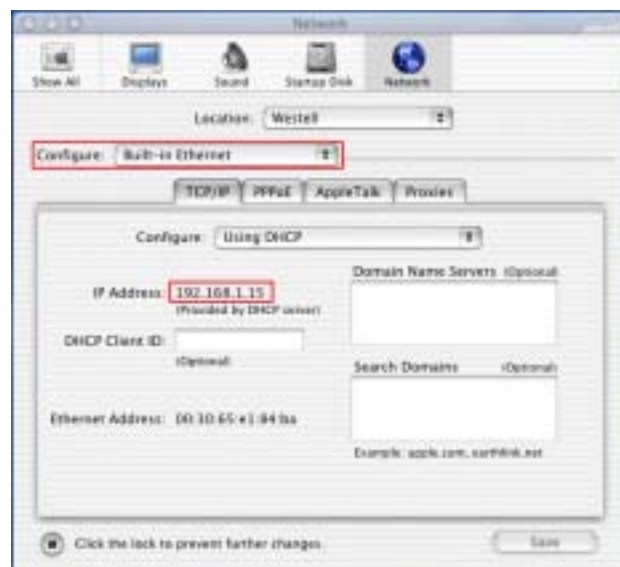


## Check the IP Connection

To verify that the computer is communicating with VersaLink, follow the instructions below.

1. Go to the “**Apple**” icon in the upper-right corner of the screen and select **System Preferences**.
2. From the **System Preferences** screen, click on the **Network** icon. The **Network** screen will be displayed.
3. From the **Configure** field in the **Network** screen, select **Built-in Ethernet**.
4. View the IP address field. An IP address that begins with **192.168.1** should be displayed.

**NOTE:** The DHCP server provides this IP address. If this IP address is not displayed, check VersaLink’s wiring connection to the PC. If necessary, refer to section 5 for hardware installation instructions.

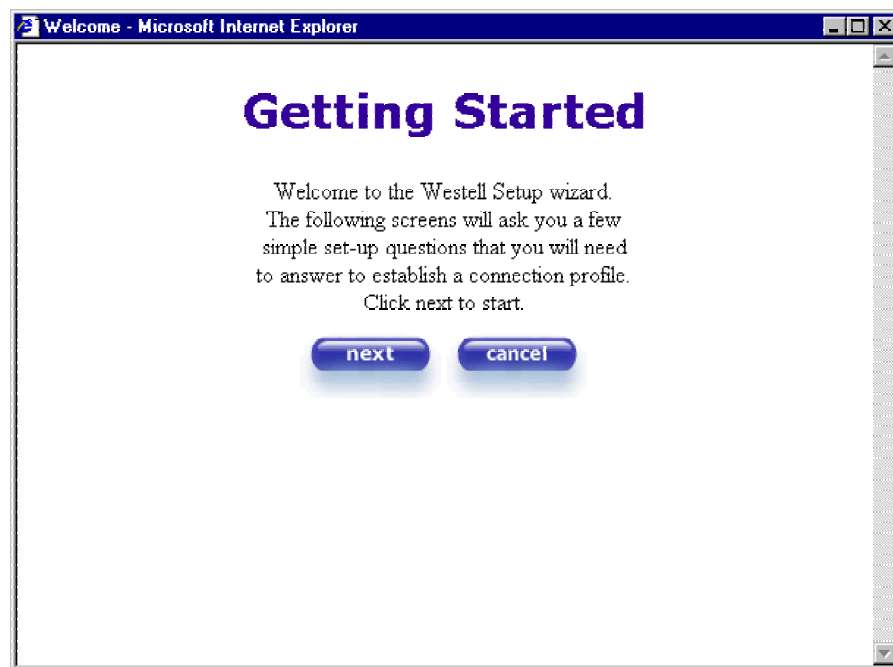


## Create a User Account

In the address window of your Internet Explorer web browser, type **http://dslrouter/**. Press 'Enter' on your keyboard.



The **Getting Started** screen will be displayed. You may now begin your Account Setup. Refer to section 7 of this User Guide to configure your Westell VersaLink for Internet connection.



**The following sections explain the advanced features of VersaLink™.**

[This Page Intentionally Left Blank]

## 9. SETTING UP ADVANCED CONFIGURATION

Advanced Configuration instructions are explained in Section 10 through Section 16. If you want to set up advanced features for VersaLink, follow the instructions provided in sections 10 through 16.

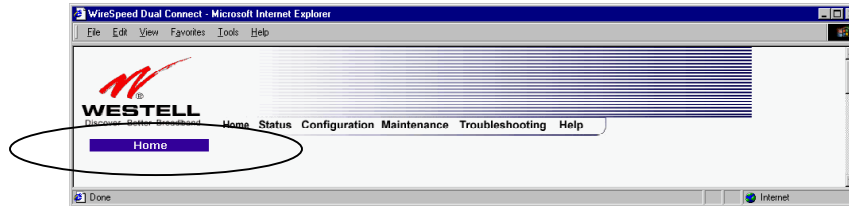
**STOP! The following sections assume that you have active DSL and Internet service.**

VersaLink™ allows you to make changes to advanced features of your Gateway such as account profiles, routing configurations, and firewall settings. The following sections explain each feature and show you how to make changes to VersaLink's settings. A menu is displayed at the top of each screen and will allow you to navigate you to the various configuration options of your VersaLink Gateway. If you are at a screen and need help, click on the **Help** button to learn more about that screen.

Please note that the menu options displayed will vary according to the WAN configuration you have chosen to use, DSLATM PORT or ETHERNET PORT1. However, all menu options are displayed when VersaLink is enabled for DSLATM PORT. Instructions on enabling and disabling DSLATM PORT and ETHERNET PORT 1 are explained in section 12.6, Advanced WAN. This document was created with the VersaLink DSLATM PORT enabled. The sections explained throughout this document will indicate when a menu item is unavailable.

## 10. HOME

As you navigate through the various screens of VersaLink, the name of the active page that you have selected will appear in the upper-left side of the screen, as shown below. Please note that the actual values may differ from the values displayed in the screens.



If you have set up your account profile and established your PPP session as discussed in section 7, the following settings will be displayed when you click on your **Home** page. Click on **profile editor** to edit your connection profile.

**NOTE:** If you have created multiple account profiles, select the option button for the active account profile.



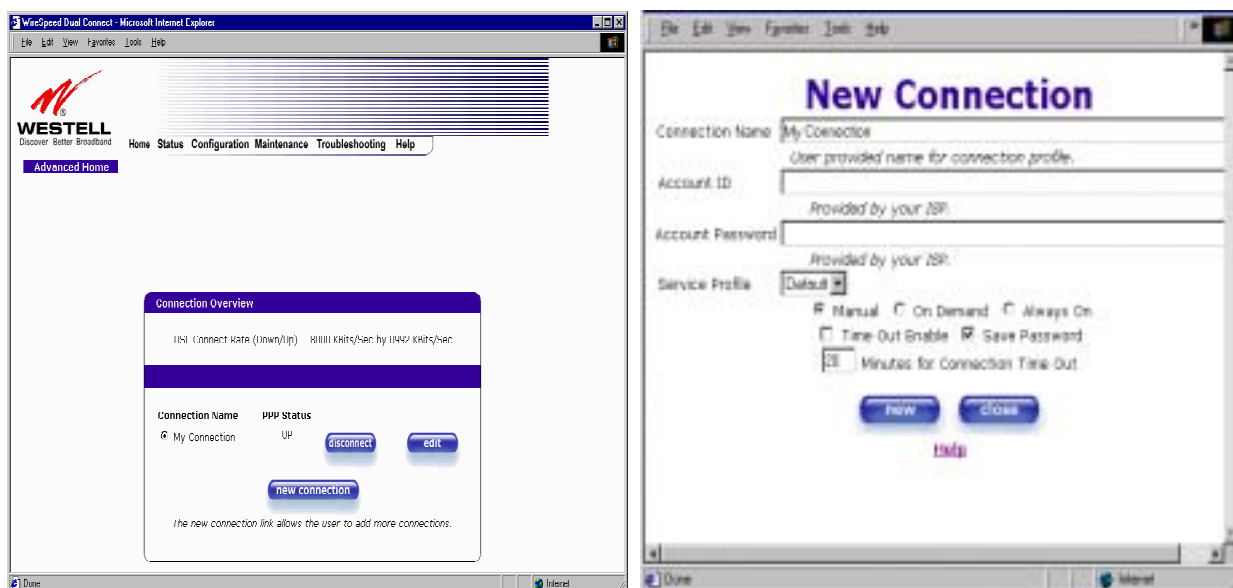
Connection Overview	Displays your DSL connection rate.
Connection Name	This Connection Name is from the connection profile that you established in section 7.
PPP Status	UP = PPP session established DOWN = No PPP session established.

Connect/Disconnect	CONNECT = Establish a PPP session DISCONNECT = Disconnect a PPP session
Profile Editor	This allows you to make changes to the profile that you created in section 7.

## 10.1 Adding Account Profiles

If you select the **Profile Editor** button from your **Home** page, the **Advanced Home** screen will appear, as shown below. Click on the **new connection** button in the **Advanced Home** screen. The **New Connection** screen will appear. Enter your account profile information and click on **New**. Next, click on **OK** in the pop-up screen to save your new connection. If you do not want to add a connection profile, click on **Close** in the **New Connection** screen.

**NOTE:** NAT Profiles allow you to create specific service settings. A NAT Profile may be associated with a certain connection setting, or NAT services. This allows you to customize the profile for specific users. You may store up to eight unique user profiles in your Gateway. Details on the **New Connection** screen are located at the end of this section.



If you clicked **OK** in the “**Save new connection?**” pop-up screen, the following screen will be displayed. This screen will allow you to edit a connection profile. Select a profile name from the **Connection Name** field and click on the **edit** button adjacent to the name.



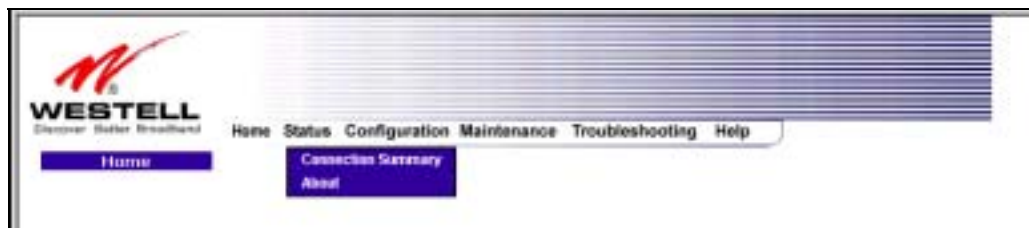
## 10.2 Editing Account Profiles

If you clicked on **Edit** in the preceding screen, the **Edit “My Connection”** screen will appear. Follow the steps in the **Edit “My Connection”** screen to change your existing connection profile, which you set up in section 7. If you do not want to change your connection profile, click on **close** in the screen. Click on **delete** if you want to delete your connection profile.



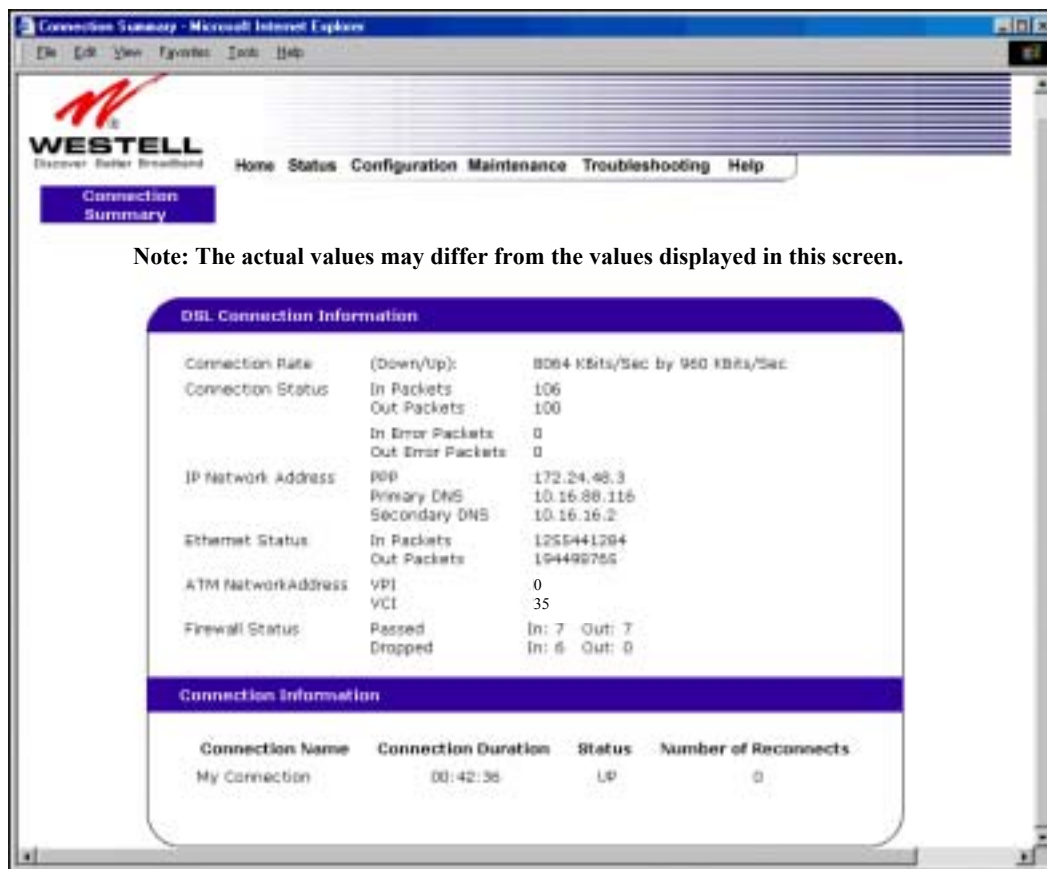
Connection Name	This field allows you to enter a new connection name of your choice (up to 64 characters).
Account ID	The account ID that you used in section 7 if you are connecting to the same Service Provider. If you have multiple Service Providers, you can enter this information at this time.
Account Password	The account password that you used in section 7 if you are connecting to the same Service Provider. If you have multiple Service Providers, you can enter this information at this time.
Service Profile	Westell recommends that you use the Default parameter.
Manual	Factory default = MANUAL Selecting this feature allows you to manually establish your PPP session.
On Demand	Selecting this feature allows the Gateway to automatically re-establish your PPP session on demand anytime your PC requests Internet activity (for example, browsing the Internet, email, etc.). When you have traffic, it may cause a delay.
Always On	Selecting this feature allows the Gateway to automatically establish a PPP session when you log on, or if the PPP session goes down.
Time Out Enable	Factory Default = DISABLED Selecting this feature allows you to enable the timeout parameter of your PPP session, which is set to a factory default of 20 minutes.
Save Password	Selecting this feature allows you to save the password for your new connection profile in VersaLink so that you will not have to re-enter it in case of a re-boot.
Minutes for Connection Time Out	This option allows you to specify the number of minutes that you want a PPP session to stay active before it is disconnected due to inactivity. (This feature works if you have selected the Time Out Enable feature explained above.)

## 11. STATUS



### 11.1 Connection Summary

The following settings will be displayed if you select **Connection Summary** from the **Status** menu.

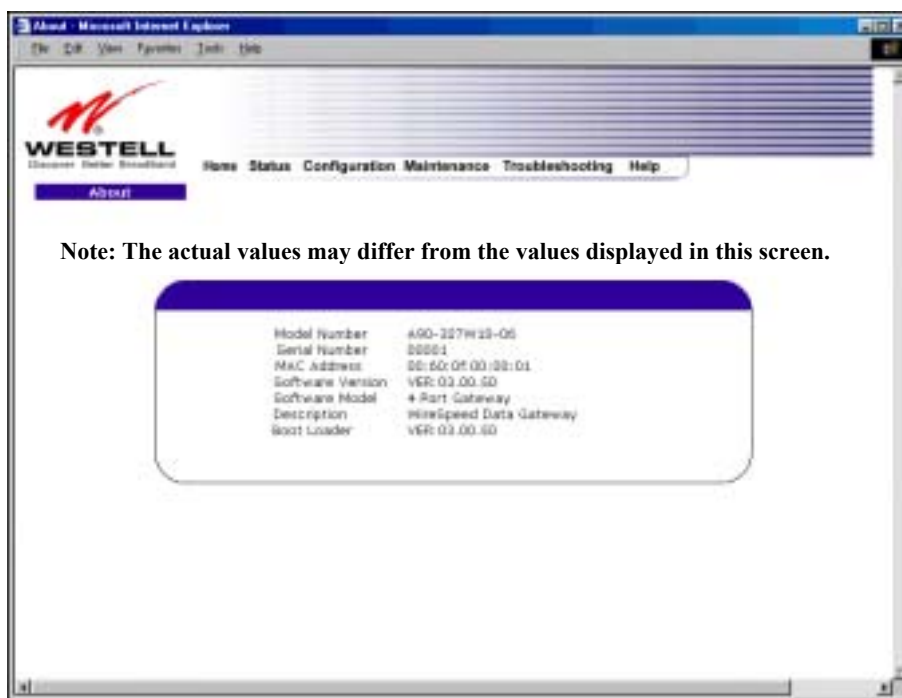


DSL Connection Information	
Connection Rate	This field will let you know if you have a DSL signal and the DSL rate at which you are connected.
Connection Status	This field will show how much information was received (IN) or sent (OUT) in packets.
IP Network Address	PPP = An IP address identifies your device on the Internet Primary DNS = Provided by your Service Provider

	Secondary DNS = Provided by your Service Provider
Ethernet Status	This field will display your Ethernet information that was received (IN) or sent (OUT) in packets on your Ethernet port.
ATM Network Address	This field will display your VPI and VCI values, which are provided by your ISP.
Firewall Status	This field will display your firewall traffic in packets. Passed: Monitors information traffic that was successfully received (IN) or transmitted (OUT) in packets. Dropped: Monitors information traffic that was not successfully received (IN) or transmitted (OUT) due to your firewall settings.
<b>PPP Connection Information</b>	
Connection Name	This is from the connection profile that you established in section 7.
Connection Duration	This field will display how long your PPP session has been connected.
Status	This field will display the status of your PPP session. UP=Connected DOWN=Disconnected
Number of Reconnects	This field will display the number of attempts that were made to establish a PPP session.

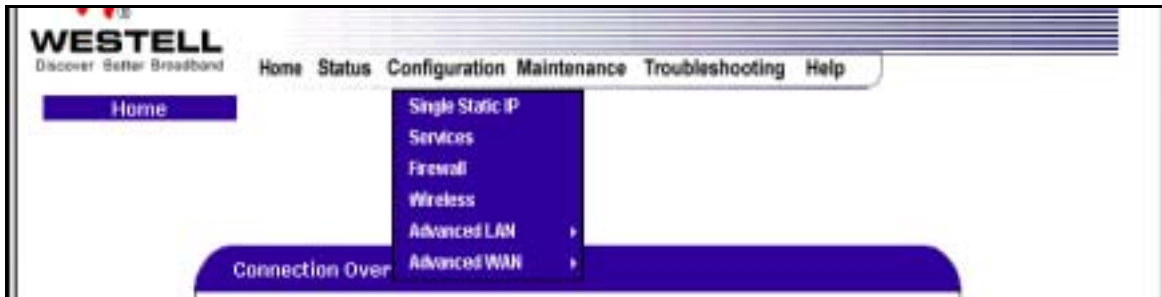
## 11.2 About

The following settings will be displayed if you select **About** from the **Status** menu.



Model Number	VersaLink manufacturer's model number.
Serial Number	VersaLink manufacturer's serial number.
MAC Address	Media Access Controller (MAC) i.e., hardware address of this device.
Software Version	Version of Application Software.
Software Model	VersaLink application type.
Description	Product description.
Boot Loader	Version of boot loader software

## 12. CONFIGURATION



### 12.1 Single Static IP – Single IP Address PassThrough

The following settings will be displayed if you select **Single Static IP** from the **Configuration** menu. The Single Static IP Configuration screen allows you to select the device on your LAN that will share your Single Static IP. Before you begin this section, configure your PC settings to obtain an IP address from your Gateway automatically. (Refer to your Windows Help screen for instructions.)

**NOTE:** Single Static IP (SSI) allows the user to share the WAN assigned IP address with one device on the LAN. By doing this, the device with the SSI becomes visible on the Internet. Network Address Translation (NAT) and Firewall rules do not apply to the device configured for SSI. If you are using Bridge (Routed Bridge) protocol, **Single Static IP** configuration will not be available.

**STOP:** Static NAT must be disabled before you can enable **Single Static IP**. To disable Static NAT, select **Services** from the **Configuration** menu. Next, click on the **static NAT** button. Select the device from the **Static NAT Device** drop-down menu and click on **disable**. Return to Single Static IP Configuration by selecting **Single Static IP Configuration** from the **Configuration** menu.



### 12.1.1 Enabling Single Static IP – Single IP Address PassThrough

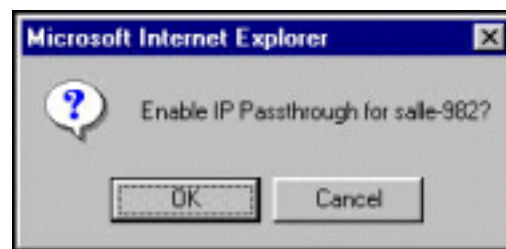
To enable Single Static IP, select a device that will share your Single Static IP from the options listed in the window. Click on **enable**.

NOTE: The Single Static IP Configuration screen allows you to select the device on your LAN that will share your Single Static IP.

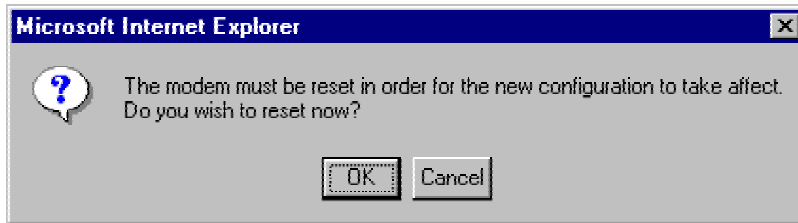


If you select a device and clicked on **enable**, the following pop-up screen will appear. Click on **OK** to enable this device for Single Static IP. Click on **Cancel** if you do not want to enable Single Static IP.

NOTE: The actual device name may differ from the name displayed in this screen.



If you clicked on **OK** in the preceding pop-up screen, the following pop-up screen will appear. VersaLink must be reset to allow the new configuration to take effect. Click on **OK**.



If you clicked on **OK** in the preceding screen, the following screen will be displayed. VersaLink will be reset and the new configuration will take effect.



After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that your PPP session displays **UP**. (Click on the **connect** button to establish a PPP session). Next, Select **Single Static IP** from the **Configuration** menu to confirm that Single Static IP is **enabled**, as shown in the following screen.



**STOP! After you enable Single Static IP, you must reboot your computer.**

**NOTE:** If you chose to enable **User Configured PC**, wait for the Gateway to reset and then manually enter the WAN IP, Gateway, and Subnet mask addresses you obtained from your Internet service provider into a PC.

## 12.1.2 Disabling Single Static IP – Single IP Address PassThrough

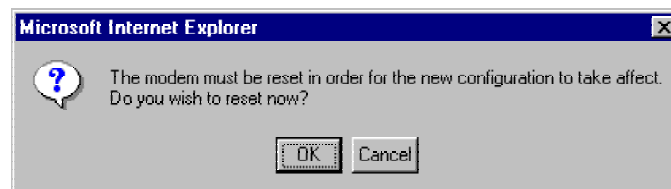
To disable Single Static IP, select **Single Static IP** from the **Configuration** menu. Click on **disable**.



If you clicked on **disable** in the preceding screen, the following pop-up screen will be displayed. Click on **OK**.



If you clicked on **OK** in the **Disable IP Passthrough?** screen, the following pop-up screen will be displayed. This screen will allow the modem to be reset and the new configuration will take effect. Click on **OK**.



If you clicked on **OK** in the preceding screen, the following screen will be displayed. VersaLink will be reset and the new configuration will take effect.



After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that your PPP session displays **UP**. (Click on the **connect** button to establish a PPP session). Next, Select **Single Static IP** from the **Configuration** menu to confirm that Single Static IP is **disabled**, as shown in the following screen.



**STOP! After you disable Single Static IP, you must reboot your computer.**

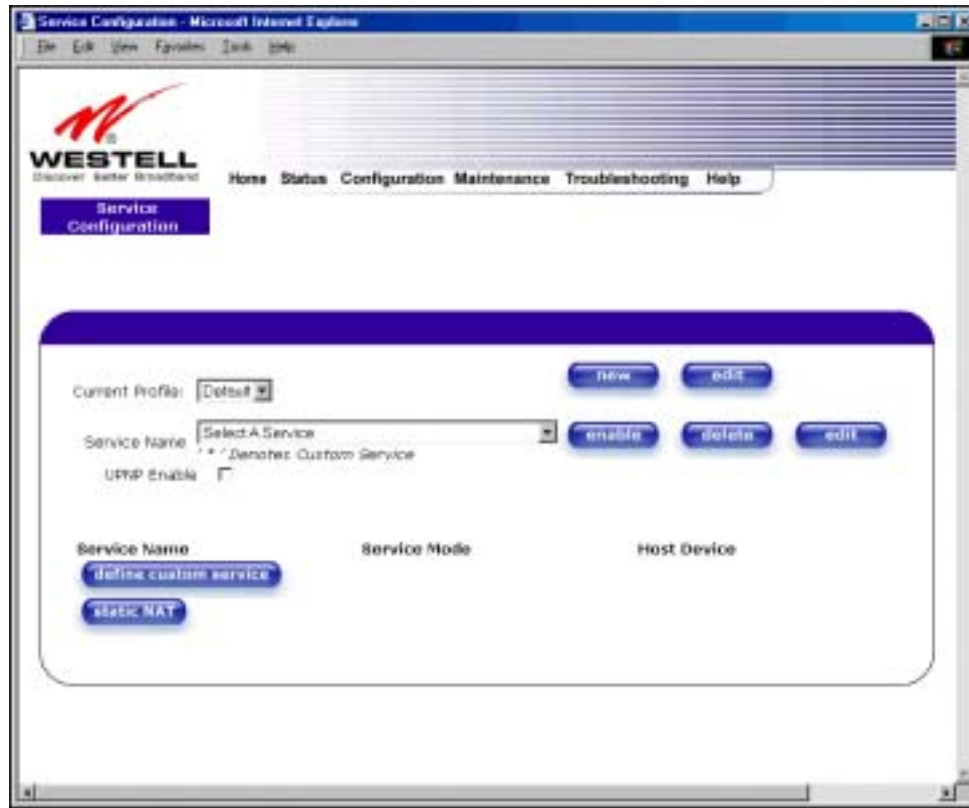
## 12.2 Service Configuration

The following settings will be displayed if you select **Services** from the **Configuration** menu.

Westell has developed an extensive list of NAT services and you may select any service from this list. By selecting your specific NAT service and setting up a NAT profile, you will ensure that the appropriate ports on VersaLink are open and that the required application traffic can pass through your LAN. For a list of supported services, go to section 16 (NAT Services).

NAT Profiles allow you to create specific service settings. The NAT profile may then be associated with a connection profile, allowing you to customize profiles for specific users. For example, if you want to attach specific NAT services to a profile, or if you want to set up a different connection setting for a profile, you can create new NAT profiles and customize them to your preference.

**NOTE:** You may create up to four NAT profiles and attach an unlimited number of services to each profile.



Current Profile	Displays the NAT (Network Address Translation) services that you have selected.
Service Name	Drop down selection menu of NAT (Network Address Translation) service you can select to configure you VersaLink.
UPNP Enable	Factory Default = Disable Enabling UPNP (Universal Plug and Play) allows automatic device discovery by your operating system.

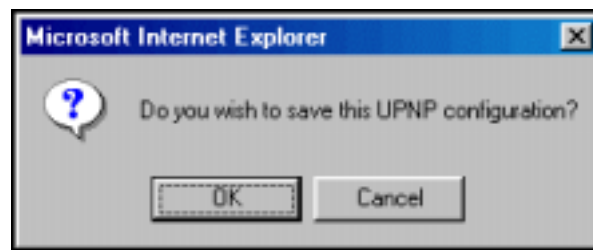
## 12.2.1 Configuring UPNP on the VersaLink

To enable UPNP on the Gateway perform the following steps:

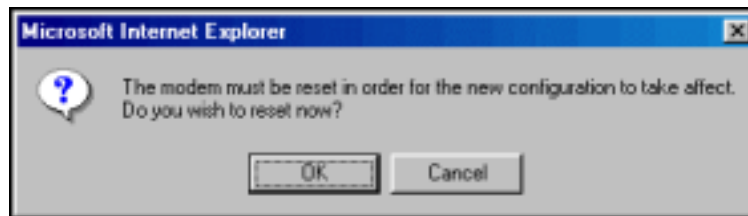
- 1) Select **Service Configuration** from the Configuration screen
- 2) Click the **UPNP Enable** box (a check mark will appear in the box).
- 3) Follow the instructions in the pop-up screens.
- 4) Click **OK** to Reset the Gateway.

**NOTE:** When you are ready to disable UPNP, uncheck the **UPNP Enable** box in the **Service Configuration** screen.

If you click the **UPNP Enable** box in the **Service Configuration** screen, a check mark will appear in the box and the following pop-up screen will be displayed. Click on **OK**.

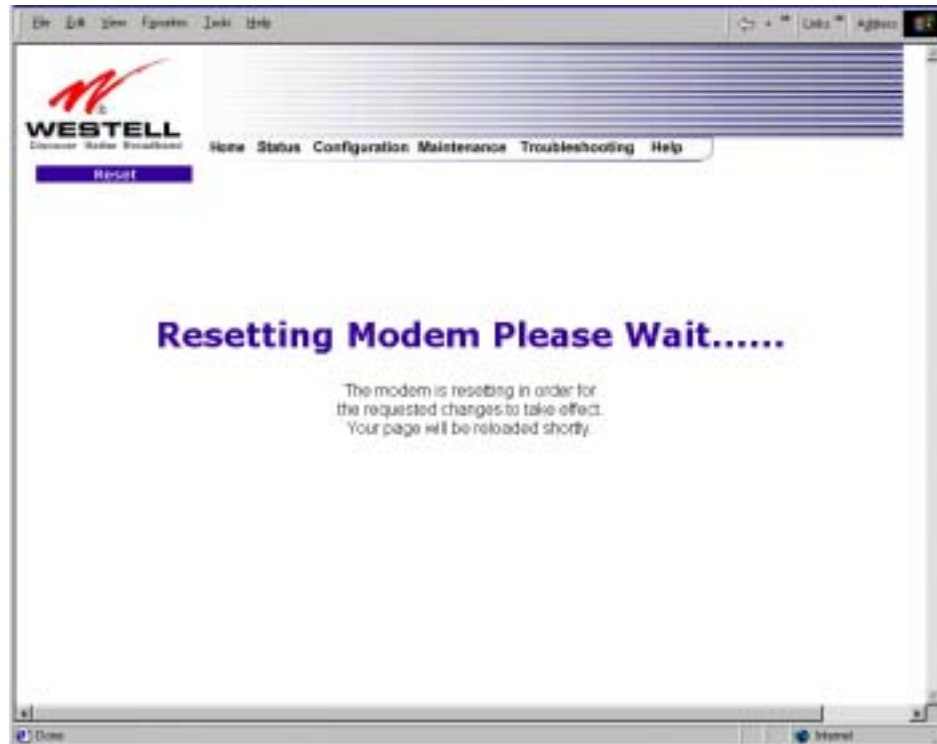


If you click **OK** in the preceding screen, the following pop-up screen will be displayed. Click on **OK** to reset the Gateway.



**Note:** To use the UPNP functionality in Versalink, your Windows XP operating system must also support UPNP. Please contact your computer manufacturer to verify that UPNP is enabled in your Windows XP operating system.

If you clicked on **OK** in the preceding screen, the following screen will be displayed. The Gateway will be reset automatically, and the new configuration will take effect.



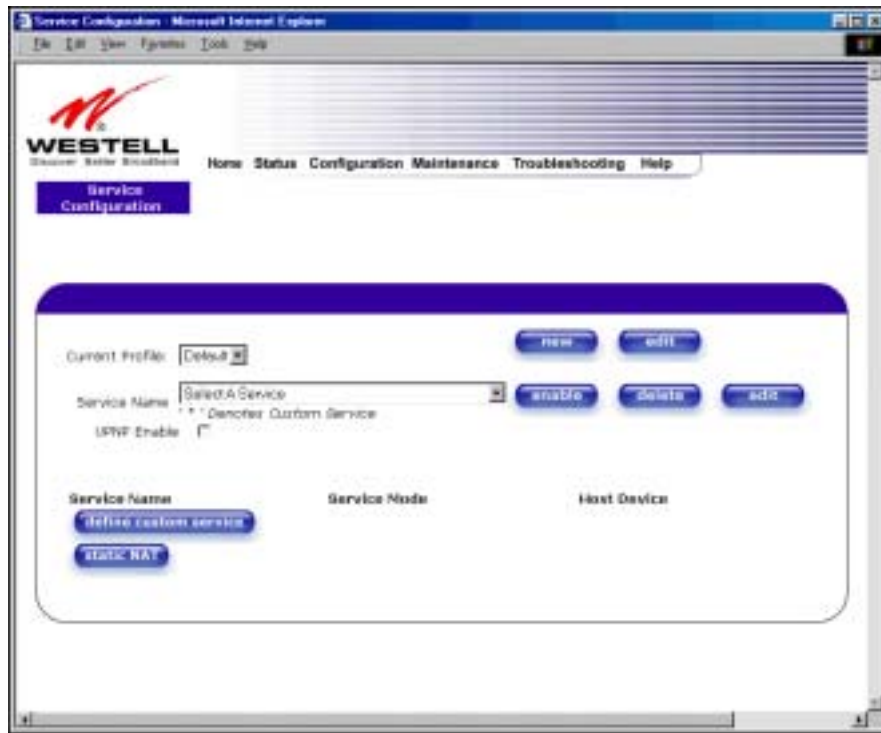
After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that your PPP session displays **UP**. (Click on the **connect** button to establish a PPP session).

## 12.2.2 Creating a New NAT Service Profile

NAT Profiles allow you to create specific service settings. The NAT profile may then be associated with a connection profile, allowing you to customize profiles for specific users. For example, if you want to attach specific NAT services to a profile, or if you want to set up a different connection setting for a profile, you can create new NAT profiles and customize them to your preference.

**NOTE:** You may create up to four NAT profiles and attach an unlimited number of services to each profile.

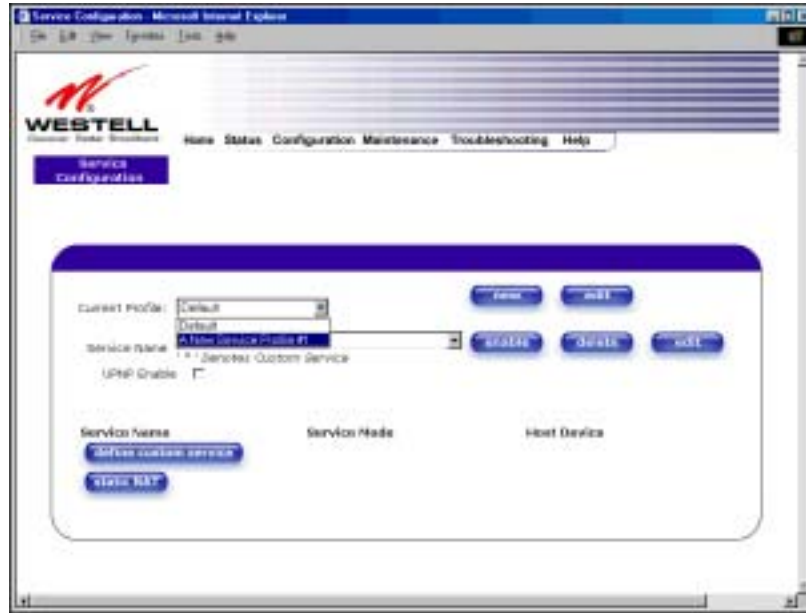
To create a new NAT profile, click **new** in the **Service Configuration** screen.



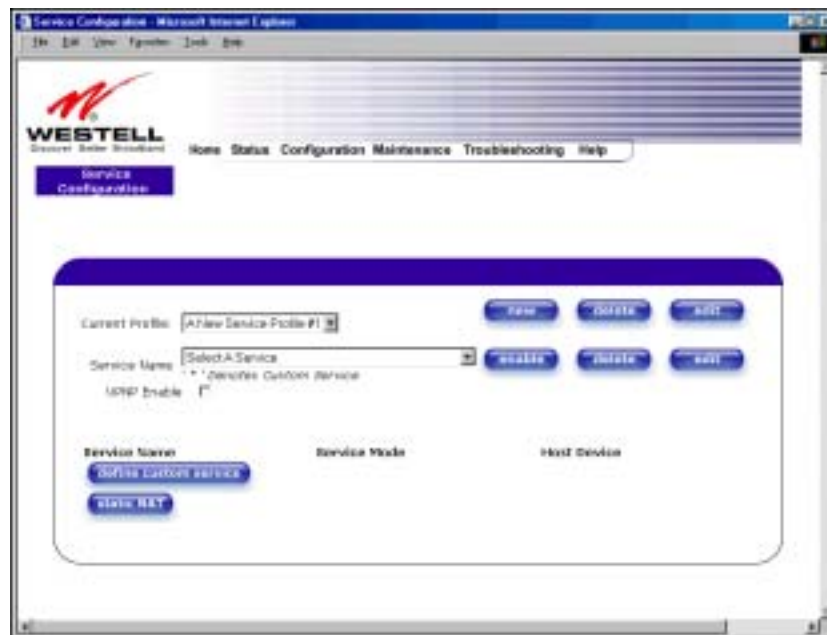
If you select **new** from the preceding **Service Configuration** screen, the **Create new Service Profile?** pop-up screen will be displayed. Click on **OK** to begin creating your new NAT service profile. Click **Cancel** if you do not want to create a new NAT service profile.



If you clicked on **OK**, the following screen will be displayed. Select **“A New Service Profile #1”** from the **Current Profile** drop-down arrow.



If you selected **“A New Service Profile #1”** from the **Current Profile** drop-down arrow, the following screen will be displayed. This screen shows that you have chosen to create a new NAT service profile. You may create up to four NAT service profiles and attach an unlimited number of services to each profile.



### 12.2.3 Editing a NAT Service Profile

After you have created a NAT service profile, you may edit the profile's name. If you select **edit** from the **Service Configuration** screen, the following screen will be displayed. By selecting the **edit** button, you can make changes to your profile name, and then, later, add to or delete NAT services from that profile. Type your new NAT service profile name in the field labeled **Profile Name**.



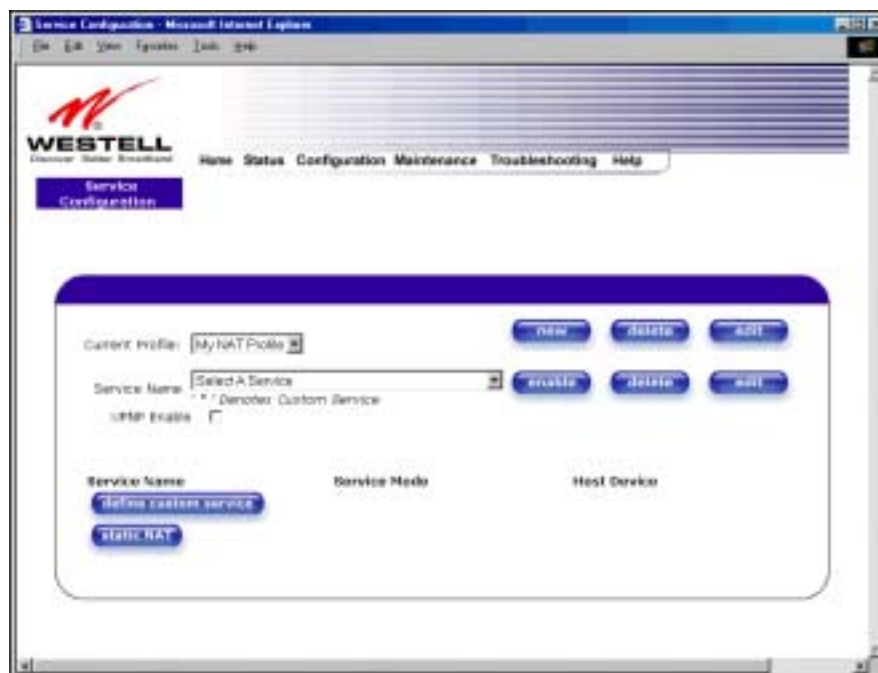
The following screen shows that a new profile name called 'My NAT Profile' was entered into the **Profile Name** field. If you want save the new NAT profile, click on **save**. If you do not want to save the new NAT profile, click on **close**.



If you clicked on **save** in the **Edit NAT Profile** screen, the following pop-up screen will be displayed. Click **OK** to save your new profile settings. If you click on **Cancel**, your new profile settings will not be saved.



The following screen displays the current profile. If desired, you may create a new profile and delete or edit an existing profile.



## 12.2.4 Adding NAT Services to a Profile

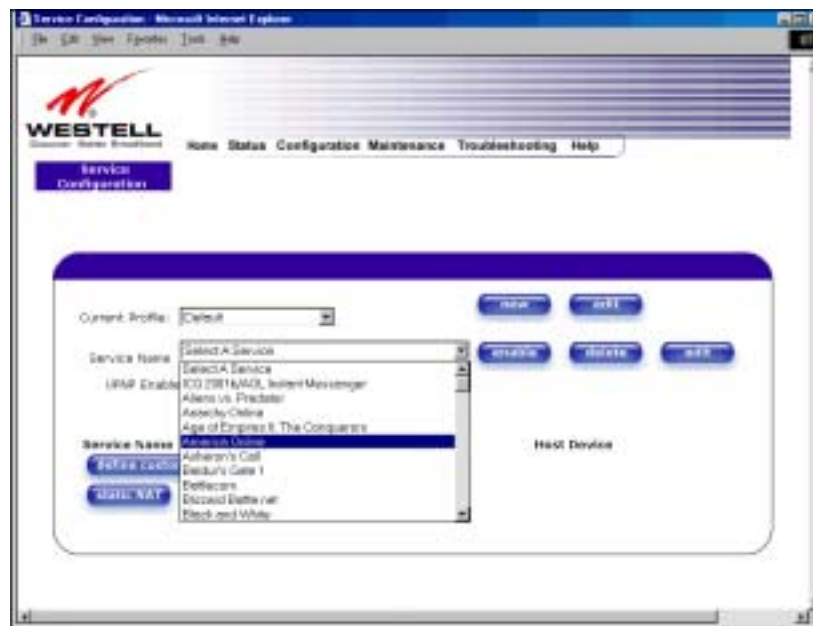
This section explains how to add NAT services to your NAT service profile. Remember, you may attach an unlimited number of NAT services to any profile.

**NOTE:** Westell has developed an extensive list of NAT services and you may select any service from this list. By selecting your specific NAT service and setting up a NAT profile, you will ensure that the appropriate ports on VersaLink are open and that the required application traffic can pass through your LAN. For a list of supported NAT services, go to section 16 (NAT Services).

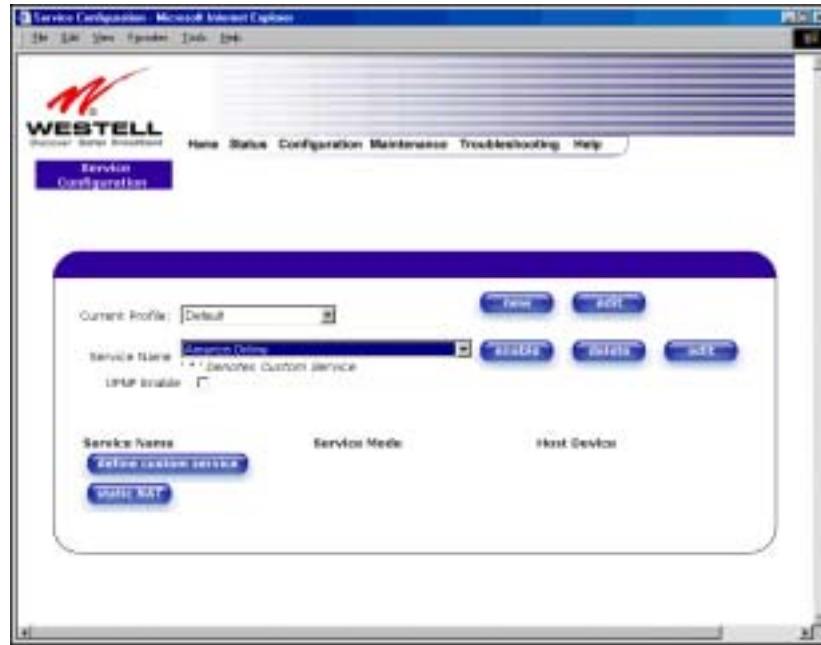
To add a NAT service, select **Services** from the **Configuration** menu. Next, Select a NAT service from the options provided at the **Service Name** drop-down arrow.

**NOTE:** You can attach multiple NAT services to your profile. However, for each NAT service that you attach to your profile, you must first select the new NAT service. Then, you must load the new NAT Configuration, as explained in section 12.2.2.

In the following screen, the 'Default' profile has been selected as the profile that will host the selected NAT service. However, you can attach a NAT service to any profile.

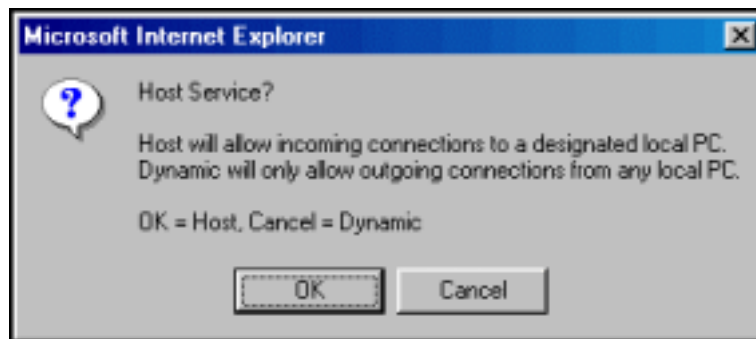


For example, the screen below displays **America Online** as the NAT service selected. After you have selected a service, click on **enable**.



If you click on **enable**, the following pop-up screen will be displayed. If you click **OK**, you will allow incoming connections to be forwarded to a designated local PC. If you click **Cancel**, you will allow only outgoing connections from any local PC. Click **OK** or click **Cancel**.

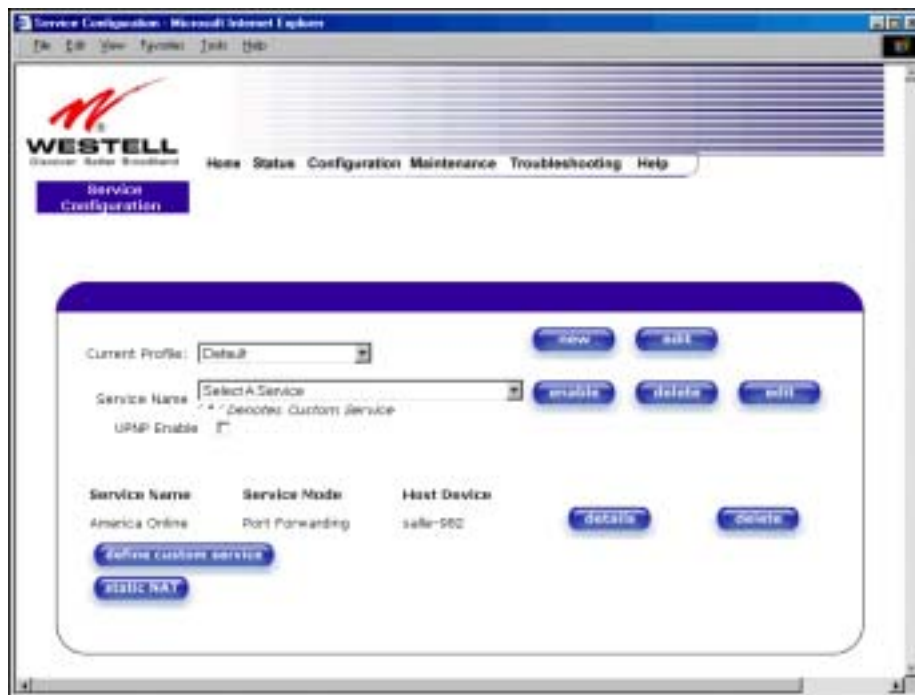
**NOTE:** If you click **Cancel** in the following pop-up screen, the NAT service you selected in the **Service Configuration** screen is still configured; however, it will not be assigned to any device on the local LAN. You must click **OK** to host the NAT service.



If you clicked on **OK** in the preceding pop-up screen, the **Host Device** screen will be displayed. The **Host Device** screen will allow you to select which device will host the NAT service you selected on your local area network. You must either select the device from the **Host Device** drop-down arrow or type an IP address in the field labeled **IP Address**. If you click on **Cancel**, the connection will be dynamically assigned. Click on **done**.



After you have selected a NAT service and you have saved it to your NAT service profile, the following screen will be displayed. It shows which NAT service is active for the selected profile.



If you select the **details** button in the **Service Configuration** screen, the following screen will display the details of the selected NAT service. If you click on the **delete** button in the **Service Configuration** screen, you will remove that NAT service from your NAT service profile. Click on **close** to continue.



NOTE: If you would like to set up additional Advanced Service Configuration options, refer to section 13 (Setting Up Advanced Service Configuration).

## 12.3 Firewall Configuration

The following settings will be displayed if you select **Firewall** from the **Configuration** menu.

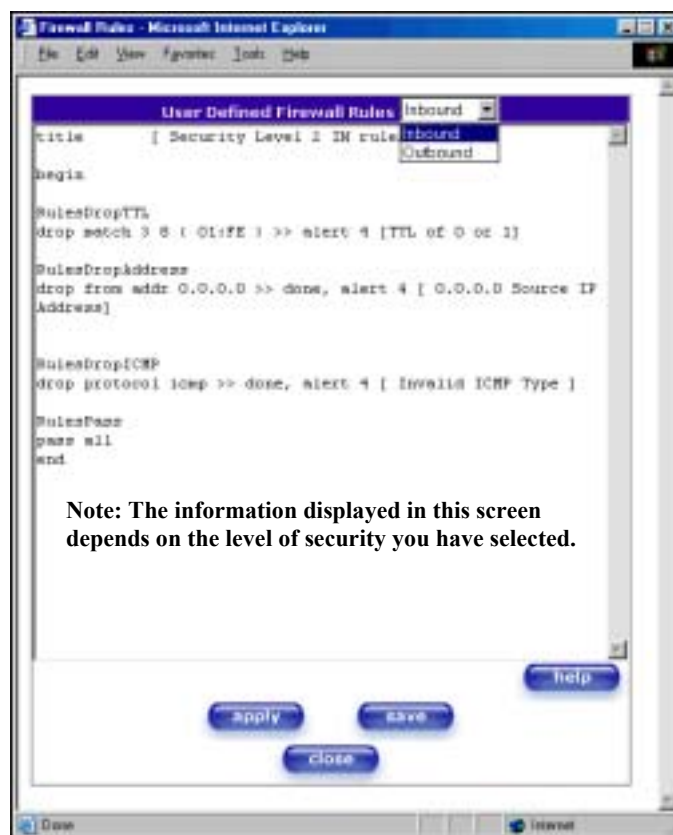


Security Level	
High	High security level only allows basic Internet functionality. Only Mail, News, Web, FTP, and IPSEC are allowed. All other traffic is prohibited.
Medium	Factory Default = MEDIUM Like High security, Medium security only allows basic Internet functionality by default. However, Medium security allows customization through NAT configuration so that you can enable the traffic that you want to pass.
Low	The Low security setting will allow all traffic except for known attacks. With Low security, VersaLink is visible to other computers on the Internet.
None	Firewall is disabled. (All traffic is passed)
Custom	Custom is an advanced configuration option that allows you to edit the firewall configuration directly. NOTE: only the most advanced users should try this.
Remote Logging	
Enable	Factory Default = Disable If enabled, Versa Link will send firewall logs to a syslog server.
Remote IP Address	The IP address of the syslog server machine to which the diagnostics logs to be sent.

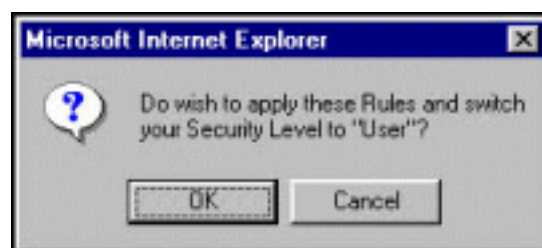
If you select **Edit** from the **Security Level** screen, the **User Defined Firewall Rules** screen will be displayed. This screen allows you to change the security parameters on your Inbound and Outbound Firewall rules via the **User Defined Firewall Rules** drop-down arrow. If you select **Inbound**, this will restrict inbound traffic from the WAN to the LAN. **Outbound** restricts outbound traffic to the WAN from the LAN. To apply the new settings, click **Apply** in the screen labeled **User Defined Firewall Rules**.

**NOTE:** Westell recommends that you do not change the settings in the **User Defined Firewall Rules** screen. If you need to reset VersaLink to factory default settings, push the reset button on the rear of VersaLink.

The information displayed in the following screen depends upon the Firewall security setting you have selected. If you selected “None” in the preceding Firewall **Security Level** screen, no values will be displayed in the following **User Defined Firewall Rules** screen.

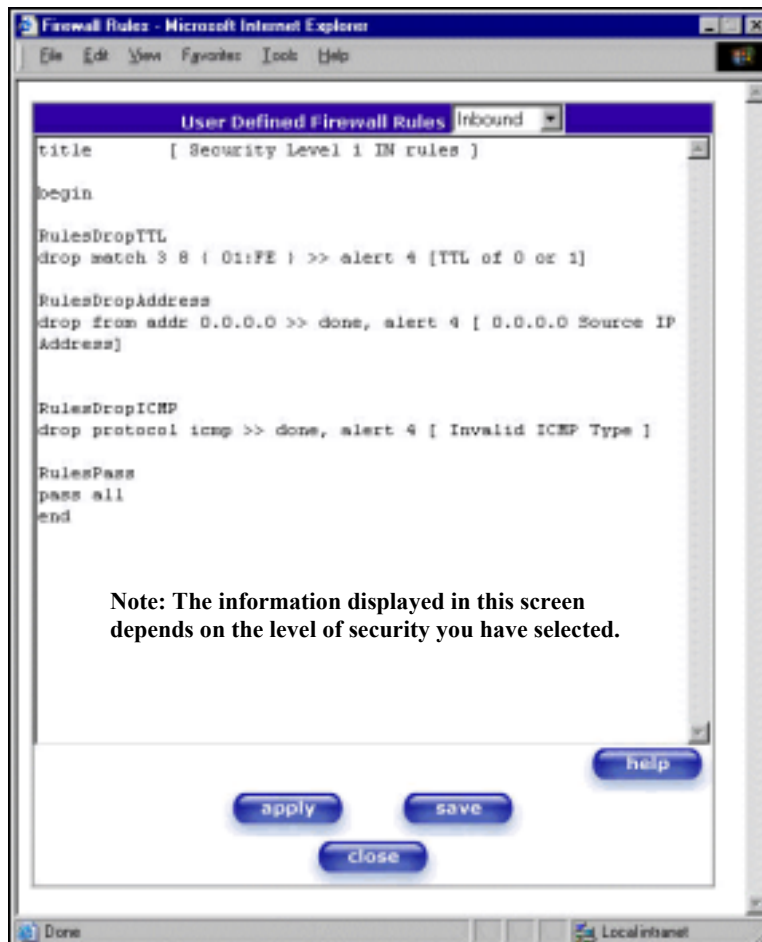


If you clicked **Apply** in the **User Define Firewall Rules** screen, the following pop-up screen will be displayed. Click on **OK** if you want your new firewall setting to take effect. If you click on **Cancel**, your new firewall settings will not take effect.



If you want to save your new firewall settings, click on **save** in the screen labeled **User Define Firewall Rules**.

**NOTE:** Westell recommends that you do not change the settings in the **User Defined Firewall Rules** screen. If you need to reset VersaLink to factory default settings, push the reset button on the rear of VersaLink.



**If you clicked save in the User Define Firewall Rules screen, the following pop-up screen will be displayed. Click OK when asked Do you wish to save these Rules to Flash and switch you Security Level to "User"? This will save your new firewall settings. If you click Cancel, your new firewall settings will not be saved.**



If you select **Help** in the screen labeled **User Defined Firewall Rules**, the following screen will be displayed. This screen gives a detailed explanation of the Firewall Rules.

**Elle/Butterfly Company**

The PDL file is a buffer format as described in section 4. The first portion of the file defines any number of types and associated values. The second portion contains the filestream definitions.

## Key Distribution Function

Key-defined constants offer key-fiddled by the macro-compiler. If value is actually a character string, the string is attempted to be open and close ranges too early. An example of a somewhat definition would look like the following:

100% (high security) (100, 100)

The dictionary engine does not use keys. This is standard practice for information associated with file. The job identifier from the key definition and value pairs are classified.

## Business Continuity

The rules within the RCL file are listed in alphabetical **length** in **word** keywords. The rules listed between these delimiters are posted and converted to a decision tree-like structure used by the packet filter engine. The rules listed are implemented sequentially as listed within RCL source. Describe posted filter engine finds a match for a rule it will rule the filter action to be taken (pass or drop) and continue to compare the following rules within given packet/headers otherwise it will rule the data packet as **deny** unless action within **deny** action within 3.2-3.2.3.

## Buffy Williams

RC4-rates may be given names. The padding/legibility facility and the user interface uses these rule names. If some applies to all rules following its declaration in the Rules section, another name is declared in the end statement. Identifier (one or more alphanumeric characters beginning with an alpha character or a line hyphen) serves as a name for the following rule.

### 804. Comments

Comments begin with hash character. The parser ignores all characters following the comment character to the end of the line.

## B04. Command Syntax

ac/PCA, communal consists of either latent indicators or another observed variable followed by one or more principal components.

FREE COACHING, COACHING !! ++ ACTUAL ACTUAL !!

The filler beyond specifies if the packet will be opened or stopped. The condition defines the position of the packet and the lid sitting to which it will be compared. The action command may specify additional objects to be taken.

**Editorial Board**

The PDL file format may be either saved or changed.

2009) show that the matching variables have entered into the associated interface of the (D/N) ratio.

**doi:** 10.1371/journal.pone.0141061.g001

### Canadian Responses

THE CONTENTS OF THIS JOURNAL ARE NOT TO BE USED FOR ANY OTHER PURPOSE

⚠ **Specifies all variables.** If all variables is specified in a rule, all other conditions are ignored.

**maxlight:off** (boolean) Specifies one or more explicit shadings and offsets into the texture space. The keywords followed by five parameters: the first parameter is the texture name, vertices index (though it differs 1, 0 = 1, 0 = 1), texture coordinates = 0. The second parameter is the offset to the texture point to the comparison. The third parameter is the comparison (the 10 shading and comparison information). The last string is determined by the open and close curly braces ("). It value defines the last string and mode. This mode is provided, a modification of all cases occurred. Each light after shading and mode is represented as a character hexadecimal number and is associated to write cases from the previous light modification.

Note: The `(IPADDR & PORTMASK)` part of `port_range == port & (PORT == PORT_M)`. Specifies particular fields (IP address or TCP/IP port numbers) of IP header. These fields are designated the source field, and the other named designated the destination field. One or more "X" descriptors of the fields and then it connects them together to represent a host ID descriptor will be replaced by values). These field descriptors include `addr` (IP address), `mask` (address mask), and `port` (TCP or UDP number).

**addr** Specifies the source or destination IP address list and comparison mask. The keyword is followed by a IP address in dotted-decimal notation and mask separated by a forward slash. The mask is a number from 1 to 32 and it signifies how many bits of the IP address are compared. If a mask is provided, a mask value of 32 is assumed.

**port** Specifies the source or destination UDP/TCP port number. This keyword is followed by the IP address and port number represented hexadecimal or decimal format. Using the `to` or `from` operators allows for matching on a range of ports.

**projection:** only **long** **angle** **value**: Specifies the value of the projection for finding the pressure. The projection is parallel to the specified **projection** value. There are four projections to the TCP, UDP, ICMP, and ICMPv6 protocols. For different **projection** values required, it can be represented by a decimal or hexadecimal value between 0 and 255.

**tcp** Specifies the TCP protocol

© 2004 Blackwell Publishing Ltd *Journal of Internal Medicine* 255: 105–112

**Example:** Suppose there is the OC-BP protocol.

**Source:** U.S. Census Bureau, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009, 2010, 2011, 2012, 2013, 2014, 2015, 2016, 2017, 2018, 2019, 2020, 2021, 2022, 2023, 2024, 2025, 2026, 2027, 2028, 2029, 2030, 2031, 2032, 2033, 2034, 2035, 2036, 2037, 2038, 2039, 2040, 2041, 2042, 2043, 2044, 2045, 2046, 2047, 2048, 2049, 2050, 2051, 2052, 2053, 2054, 2055, 2056, 2057, 2058, 2059, 2060, 2061, 2062, 2063, 2064, 2065, 2066, 2067, 2068, 2069, 2070, 2071, 2072, 2073, 2074, 2075, 2076, 2077, 2078, 2079, 2080, 2081, 2082, 2083, 2084, 2085, 2086, 2087, 2088, 2089, 2090, 2091, 2092, 2093, 2094, 2095, 2096, 2097, 2098, 2099, 2100, 2101, 2102, 2103, 2104, 2105, 2106, 2107, 2108, 2109, 2110, 2111, 2112, 2113, 2114, 2115, 2116, 2117, 2118, 2119, 2120, 2121, 2122, 2123, 2124, 2125, 2126, 2127, 2128, 2129, 2130, 2131, 2132, 2133, 2134, 2135, 2136, 2137, 2138, 2139, 2140, 2141, 2142, 2143, 2144, 2145, 2146, 2147, 2148, 2149, 2150, 2151, 2152, 2153, 2154, 2155, 2156, 2157, 2158, 2159, 2160, 2161, 2162, 2163, 2164, 2165, 2166, 2167, 2168, 2169, 2170, 2171, 2172, 2173, 2174, 2175, 2176, 2177, 2178, 2179, 2180, 2181, 2182, 2183, 2184, 2185, 2186, 2187, 2188, 2189, 2190, 2191, 2192, 2193, 2194, 2195, 2196, 2197, 2198, 2199, 2200, 2201, 2202, 2203, 2204, 2205, 2206, 2207, 2208, 2209, 2210, 2211, 2212, 2213, 2214, 2215, 2216, 2217, 2218, 2219, 2220, 2221, 2222, 2223, 2224, 2225, 2226, 2227, 2228, 2229, 2230, 2231, 2232, 2233, 2234, 2235, 2236, 2237, 2238, 2239, 2240, 2241, 2242, 2243, 2244, 2245, 2246, 2247, 2248, 2249, 2250, 2251, 2252, 2253, 2254, 2255, 2256, 2257, 2258, 2259, 2260, 2261, 2262, 2263, 2264, 2265, 2266, 2267, 2268, 2269, 2270, 2271, 2272, 2273, 2274, 2275, 2276, 2277, 2278, 2279, 2280, 2281, 2282, 2283, 2284, 2285, 2286, 2287, 2288, 2289, 2290, 2291, 2292, 2293, 2294, 2295, 2296, 2297, 2298, 2299, 2300, 2301, 2302, 2303, 2304, 2305, 2306, 2307, 2308, 2309, 2310, 2311, 2312, 2313, 2314, 2315, 2316, 2317, 2318, 2319, 2320, 2321, 2322, 2323, 2324, 2325, 2326, 2327, 2328, 2329, 2330, 2331, 2332, 2333, 2334, 2335, 2336, 2337, 2338, 2339, 2340, 2341, 2342, 2343, 2344, 2345, 2346, 2347, 2348, 2349, 2350, 2351, 2352, 2353, 2354, 2355, 2356, 2357, 2358, 2359, 2360, 2361, 2362, 2363, 2364, 2365, 2366, 2367, 2368, 2369, 2370, 2371, 2372, 2373, 2374, 2375, 2376, 2377, 2378, 2379, 2380, 2381, 2382, 2383, 2384, 2385, 2386, 2387, 2388, 2389, 2390, 2391, 2392, 2393, 2394, 2395, 2396, 2397, 2398, 2399, 2400, 2401, 2402, 2403, 2404, 2405, 2406, 2407, 2408, 2409, 2410, 2411, 2412, 2413, 2414, 2415, 2416, 2417, 2418, 2419, 2420, 2421, 2422, 2423, 2424, 2425, 2426, 2427, 2428, 2429, 2430, 2431, 2432, 2433, 2434, 2435, 2436, 2437, 2438, 2439, 2440, 2441, 2442, 2443, 2444, 2445, 2446, 2447, 2448, 2449, 2450, 2451, 2452, 2453, 2454, 2455, 2456, 2457, 2458, 2459, 2460, 2461, 2462, 2463, 2464, 2465, 2466, 2467, 2468, 2469, 2470, 2471, 2472, 2473, 2474, 2475, 2476, 2477, 2478, 2479, 2480, 2481, 2482, 2483, 2484, 2485, 2486, 2487, 2488, 2489, 2490, 2491, 2492, 2493, 2494, 2495, 2496, 2497, 2498, 2499, 2500, 2501, 2502, 2503, 2504, 2505, 2506, 2507, 2508, 2509, 2510, 2511, 2512, 2513, 2514, 2515, 2516, 2517, 2518, 2519, 2520, 2521, 2522, 2523, 2524, 2525, 2526, 2527, 2528, 2529, 2530, 2531, 2532, 2533, 2534, 2535, 2536, 2537, 2538, 2539, 2540, 2541, 2542, 2543, 2544, 2545, 2546, 2547, 2548, 2549, 2550, 2551, 2552, 2553, 2554, 2555, 2556, 2557, 2558, 2559, 2560, 2561, 2562, 2563, 2564, 2565, 2566, 2567, 2568, 2569, 2570, 2571, 2572, 2573, 2574, 2575, 2576, 2577, 2578, 2579, 2580, 2581, 2582, 2583, 2584, 2585, 2586, 2587, 2588, 2589, 2590, 2591, 2592, 2593, 2594, 2595, 2596, 2597, 2598, 2599, 2600, 2601, 2602, 2603, 2604, 2605, 2606, 2607, 2608, 2609, 2610, 2611, 2612, 2613, 2614, 2615, 2616, 2617, 2618, 2619, 2620, 2621, 2622, 2623, 2624, 2625, 2626, 2627, 2628, 2629, 2630, 2631, 2632, 2633, 2634, 2635, 2636, 2637, 2638, 2639, 2640, 2641, 2642, 2643, 2644, 2645, 2646, 2647, 2648, 2649, 2650, 2651, 2652, 2653, 2654, 2655, 2656, 2657, 2658, 2659, 2660, 2661, 2662, 2663, 2664, 2665, 2666, 2667, 2668, 2669, 2670, 2671, 2672, 2673, 2674, 2675, 2676, 2

**PLEASE NOTE:** ONLY 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115, 116, 117, 118, 119, 120, 121, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 135, 136, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 154, 155, 156, 157, 158, 159, 160, 161, 162, 163, 164, 165, 166, 167, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 178, 179, 180, 181, 182, 183, 184, 185, 186, 187, 188, 189, 190, 191, 192, 193, 194, 195, 196, 197, 198, 199, 200, 201, 202, 203, 204, 205, 206, 207, 208, 209, 210, 211, 212, 213, 214, 215, 216, 217, 218, 219, 220, 221, 222, 223, 224, 225, 226, 227, 228, 229, 230, 231, 232, 233, 234, 235, 236, 237, 238, 239, 240, 241, 242, 243, 244, 245, 246, 247, 248, 249, 250, 251, 252, 253, 254, 255, 256, 257, 258, 259, 260, 261, 262, 263, 264, 265, 266, 267, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 304, 305, 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 360, 361, 362, 363, 364, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 387, 388, 389, 390, 391, 392, 393, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 409, 410, 411, 412, 413, 414, 415, 416, 417, 418, 419, 420, 421, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 435, 436, 437, 438, 439, 440, 441, 442, 443, 444, 445, 446, 447, 448, 449, 450, 451, 452, 453, 454, 455, 456, 457, 458, 459, 460, 461, 462, 463, 464, 465, 466, 467, 468, 469, 470, 471, 472, 473, 474, 475, 476, 477, 478, 479, 480, 481, 482, 483, 484, 485, 486, 487, 488, 489, 490, 491, 492, 493, 494, 495, 496, 497, 498, 499, 500, 501, 502, 503, 504, 505, 506, 507, 508, 509, 510, 511, 512, 513, 514, 515, 516, 517, 518, 519, 520, 521, 522, 523, 524, 525, 526, 527, 528, 529, 530, 531, 532, 533, 534, 535, 536, 537, 538, 539, 540, 541, 542, 543, 544, 545, 546, 547, 548, 549, 550, 551, 552, 553, 554, 555, 556, 557, 558, 559, 560, 561, 562, 563, 564, 565, 566, 567, 568, 569, 570, 571, 572, 573, 574, 575, 576, 577, 578, 579, 580, 581, 582, 583, 584, 585, 586, 587, 588, 589, 590, 591, 592, 593, 594, 595, 596, 597, 598, 599, 600, 601, 602, 603, 604, 605, 606, 607, 608, 609, 610, 611, 612, 613, 614, 615, 616, 617, 618, 619, 620, 621, 622, 623, 624, 625, 626, 627, 628, 629, 630, 631, 632, 633, 634, 635, 636, 637, 638, 639, 640, 641, 642, 643, 644, 645, 646, 647, 648, 649, 650, 651, 652, 653, 654, 655, 656, 657, 658, 659, 660, 661, 662, 663, 664, 665, 666, 667, 668, 669, 670, 671, 672, 673, 674, 675, 676, 677, 678, 679, 680, 681, 682, 683, 684, 685, 686, 687, 688, 689, 690, 691, 692, 693, 694, 695, 696, 697, 698, 699, 700, 701, 702, 703, 704, 705, 706, 707, 708, 709, 710, 711, 712, 713, 714, 715, 716, 717, 718, 719, 720, 721, 722, 723, 724, 725, 726, 727, 728, 729, 730, 731, 732, 733, 734, 735, 736, 737, 738, 739, 740, 741, 742, 743, 744, 745, 746, 747, 748, 749, 750, 751, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 762, 763, 764, 765, 766, 767, 768, 769, 770, 771, 772, 773, 774, 775, 776, 777, 778, 779, 780, 781, 782, 783, 784, 785, 786, 787, 788, 789, 790, 791, 792, 793, 794, 795, 796, 797, 798, 799, 800, 801, 802, 803, 804, 805, 806, 807, 808, 809, 810, 811, 812, 813, 814, 815, 816, 817, 818, 819, 820, 821, 822, 823, 824, 825, 826, 827, 828, 829, 830, 831, 832, 833, 834, 835, 836, 837, 838, 839

**type type query report** Simulates the GMP analysis tool for the GMP module. The **report** type checks for information 1 and version 1 type codes. No check is made by the parser to verify that the GMP protocol is specified. In this case the user is notified by the **protocol type** condition in order to verify the type type condition.

**Non-governmental roles:** Identified by IMF (2004) and by IMF (2006). No check is made by the private bank for the IMF's policies specified. Not tied to the user but to the **publications** condition and role using the **comp** role condition.

## Artigos Imprescindíveis

Specification (iii) reflects the fact that the probability of a match between the rule condition and the object's content

**log\_level** Specifies the log contents of any matching partial header should be recorded in the log table. The level parameter is a mechanism to indicate the source of the log entry. This value subname is stored with auditing entry resulting from this rule. The logname subsequently be searched or sorted by the source rule name. Log entries appear in the table with a default priority of 0. The user value is represented as a value of 0 to 1000 to indicate the priority of the rule. 0 and 1000.

**test\_severity(test\_name)** Specifies that the contents of any subsequence headers should be recorded under separate sub-headers for corresponding severity values and sub-explanation. Severity is a decimal number between 0 and 5. The classification is defined by `enumSeverity` in the `test` test.

**Issue:** Specifier that the Mongo engine should stop the rule any subsequent rules should the rule match. The action provides some metadata regarding the decision the command made to the Mongo engine.

**State** Species filter: TPCBP/PCBP (concatenate state filter sequence number in the case of TCF and the post filter and exon-intron/alternative address and analysis filter case of CDP and CDP) associated with this post filter will add to the state table maintained by the filtering engine. In case of this concat operation, the state table will contain all entries associated with the previous post filter concatenated with the state filter case. The filtering engine will take logs containing the state of the second with the second post filter and second filter case between them. The state table, whenever accessed,

## 12.4 Wireless Configuration

The following fields will be displayed if you select **Wireless** from the **Configuration** menu.

**IMPORTANT:** If you are connecting to VersaLink via a wireless network adapter, the service set ID (SSID) must be the same for both the Westell VersaLink and your PC's wireless network adapter. The default SSID for VersaLink is the serial number of the unit (located below the bar code on the bottom of the unit and also on the Westell shipping carton). Locate and run the utility software provided with your PC's Wireless network adapter and enter the SSID value. The PC's wireless network adapter must be configured with the SSID (in order to communicate with VersaLink) before you begin VersaLink's account setup and configuration procedures. For privacy, you may change the **Network Name (SSID)** value in the **Wireless Configuration** screen to your desired value.

NOTE: Client PCs can use any Wireless Fidelity (Wi-Fi) 802.11b/g+ certified card to communicate with VersaLink. The Wireless card and VersaLink must use the same Wired Equivalent Privacy (WEP) security code type. The factory default for WEP is DISABLED. If you enable WEP, you must ensure the network setting for your wireless adapter is set to "Must Use Shared Key for WEP" or "Open Wi-Fi." You must ensure that your PC's Wi-Fi adapter is configured properly for whichever network setting you use. You can access the settings in the advanced properties of the wireless network adapter.

To select a network setting, click on the drop-down arrow at the field labeled **Authentication Type**, and then select either **Open System** or **Shared Key**. If you change any settings in this screen, you must click on the **Save** button to ensure that the settings take effect.

NOTE: For privacy, you should change the **Network Name (SSID)** value to your desired value.



<b>Wireless Card Information</b>	
Wireless Operation	Factory Default = Enabled. When disabled, no stations will be able to connect to the VersaLink.
Network Name (SSID)	This string, (32 characters or less) is the name associated with the AP. To connect to the AP, the SSID on a Station card must match the SSID on the AP card or be set to "ANY."
Channel	The AP transmits and receives data on this channel. The number of channels to choose from is pre-programmed into the AP card. Station cards do not have to be set to the same channel as the AP; the Stations scan all channels, and look for an AP to connect to.
Mode	This setting allows station to communicate with VersaLink.  Possible Responses: Mixed: Station using any of the 802.11b, 802.11b+, and 802.11g rates can communicate with VersaLink. 11b only: Communication with VersaLink is limited to 802.11b <b>11b+</b> : Stations using any of the 802.11b and 802.11b+ rates can communicate with VersaLink 11g only: Communication with VersaLink is limited to 802.11g
4x Support	Factory Default = Disabled When selected, this enables/disables the 4X option. If enabled, 4X support provides additional algorithms for increased throughput. The station cards must also support this option.
Advanced Configuration edit button	Selecting this button allows access to the Wireless Advanced Configuration settings.
<b>Privacy Settings</b>	
Authentication Type	Factory Default = Open System Possible Response: Open System: Open System authentication is the default selection. Shared Key: To use Shared Key authentication, WEP must be enabled, and a valid WEP key must be present. Enabling WEP does not force the use of Shared Key authentication. It is permissible to have WEP enabled and still use Open System authentication.
WEP Security WEP Security WEP (Wired Equivalent Privacy)	Factory Default=DISABLED The AP card supports 64-bit, 128-bit, or 256-bit WEP encryption. If WEP is disabled, any station can connect to the AP (as long as its SSID matches the AP SSID). IF WEP is enabled, the risk of someone nearby accessing the AP is minimized.
Key Select	If selected, the WEP Key is treated as a string of text characters, and the number of characters must be either 5 (for 64-bit encryption) or 13 (for 128-bit encryption) or 29 (for 256-bit encryption). If not selected, the WEP key is treated as a string of hexadecimal characters, and the number of characters must be either 10 (for 64-bit encryption), 26 (for 128-bit encryption), or 58 (for 256-bit encryption). The only allowable hexadecimal characters are 0-9 and A-F. NOTE: The WEP key must be the same value and type for both VersaLink and the wireless network adapter. "Pass Phrase" is not the same as "text" and should not be used.
Key Mapping Table button	Selecting this button will allows access to the Wireless Key Mappings settings.
Hide SSID	Factory Default = Disabled. If Enabled, Versa Link will not broadcast the SSID. Stations must configure the SSID to match the Network Name (SSID) to connect to VersaLink.
MAC Address Filtering	Factory Default = Disabled. If Enabled, only the stations in the MAC Filter Table can connect to VersaLink.
MAC Filter Table button	Selecting this button allows access to the Wireless MAC Address Filter Table.

## 12.4.1 Wireless Advanced Configuration

The following screen will be displayed if you click on the **edit** button adjacent to **Advanced Configuration** in the **Wireless Configuration** screen.

The screenshot shows the 'Wireless Advanced Configuration' screen. At the top, there is a navigation bar with links: Home, Status, Configuration, Maintenance, Troubleshooting, and Help. Below this is a sub-header 'Wireless Advanced Configuration'. The main configuration area contains the following settings:

- Beacon Period:** 288 msecs (range: 1-65536)
- RTS Threshold:** 2347 bytes (range: 0-2347)
- Fragmentation Threshold:** 2346 bytes (range: 256-2346)
- Preamble Algorithm:** Local STA's
- Slot Time Algorithm:** Local STA's
- PCC Algorithm:** Enhanced Dynamic
- ERP Protection Algorithm:** Dynamic
- Rate Adaptation:** Enabled
- Rate Fallback:** After 1 Retry
- 802.11b Rates(Mbps):** N - not supported, Y - supported, B - basic supported. Values: 1, 2, 5.5, 11, 22.
- 802.11g Rates(Mbps):** N - not supported, Y - supported, B - basic supported. Values: 6, 9, 12, 18, 24, 36, 48, 54.

At the bottom of the configuration area are three buttons: Save, Cancel, and Back.

Beacon Period	The time interval between beacon frame transmissions. Beacons contain rate and capability information. Beacons received by stations can be used to identify the access points in the area.
RTS Threshold	RTS/CTS handshaking will be performed for any data or management MPDU containing a number of bytes greater than the threshold. If this value is larger than the MSDU size (typically set by the fragmentation threshold), no handshaking will be performed. A value of zero will enable handshaking for all MPDUs.
Fragmented Threshold	Any MSDU or MMPDU larger than this value will be fragmented into an MPDU of the specified size.
Preamble Algorithm	Factory Default = Local STA's Possible Responses: Always Long: Transmissions are done using the long preamble algorithm. Always Short: Transmissions are done using the short preamble algorithm. Local STA's: If all associated stations support short preamble, then the short preamble algorithm is used. Otherwise, the long preamble algorithm is used.
Slot Time Algorithm	Factory Default = Local STA's  Possible Response: Always Off: Transmissions are done using a 20 usec slot time.

	<p>Always ON: Transmissions are done using a usec slot time (SST).</p> <p>Local STA's: If all associated stations support SST, then the 9 usec slot time is used. Otherwise, the 20 uses slot time is used.</p> <p>Enhanced Dynamic: Similar to Local STA's, with the following extension: If associated stations that do not support SST do not transmit for a period of time, the 9 usec slot time is used.</p>
PBCC Algorithm	<p>Factory Default = Enhanced Dynamic</p> <p>Possible Response:</p> <p>Always Off: PBCC is not used, operation at 22 Mbps is not possible.</p> <p>Always ON: PBCC is used.</p> <p>Local STA's: If all associated stations support PBCC, then PBCC is used. Otherwise, PBCC is not used.</p> <p>Dynamic: Similar to local STA's with the following extension: PBCC setting is also dependent on Beacon frames from overlapping BSS. If Beacon frames are received that do not support PBCC, then PBCC is not used.</p> <p>Enhanced Dynamic: Similar to Dynamic with the following extension: If associated stations that do not support PBCC do not transmit for a period of time, then PBCC is not used.</p>
ERP Protection Algorithm	<p>Factory Default = Dynamic</p> <p>Possible Response:</p> <p>Always Off: ERP is not used</p> <p>Always ON: ERP is used.</p> <p>Local STA's: If there are any associated stations than do not support ERP, a protection algorithm is used to prevent contention.</p> <p>Dynamic: Similar to local STA's with the following extension: The ERP protection setting is also dependent on Beacon frames from overlapping BSS. IF Beacon frames are received that indicate ERP is not supported, then a protection algorithm is used.</p> <p>Enhanced Dynamic: Similar to Dynamic with the following extension: If associated stations that do not support ERP do not transmit for a period of time, then protection algorithm is not used.</p>
Rate Adaptation	<p>Factory Default = Enable</p> <p>If disabled, the highest rate shared between VersaLink and STA is used for each transmission.</p>
Rate Fallback	<p>Factory Default = After 1 Retry</p> <p>The number of retries to attempt before falling back to the next lower rate. If Fallback is disabled, the starting rate is the only rate tried. IF Rate Adaptation is also disabled, the maximum rate shared with the STA is always the starting rate and the only rate tried. This may not work in noisy environments, and will reduce roaming distances.</p> <p>Possible Response: After 1 Retry/ Disable/ After 1 Retry/ After 2 Retry</p>
802.11b Rates (Mbps) 802.11g Rates (Mbps)	<p>These are the allowable communication rates that VersaLink will attempt to use. The rates are also broadcast within the connection protocol as the rates supported by VersaLink.</p>

## 12.4.2 Wireless Key Mappings

The following screen will be displayed if you click on the **edit** button adjacent to **Key Mapping Table** in the **Wireless Configuration** screen.



WEP Key	Select Enable if you want this WEP key enabled for the listed MAC Address.
MAC Address	The MAC address assigned to the station for which you want to assign a WEP key.
Key Length	The number of bits the encryption is going to use for WEP. The options are 64, 128, or 256 bits.
Key Value	The WEP key to be used for this station.

### 12.4.3 Wireless Filter Table

The following screen will be displayed if you click on the **edit** button adjacent to **MAC Filter Table** in the **Wireless Configuration** screen.

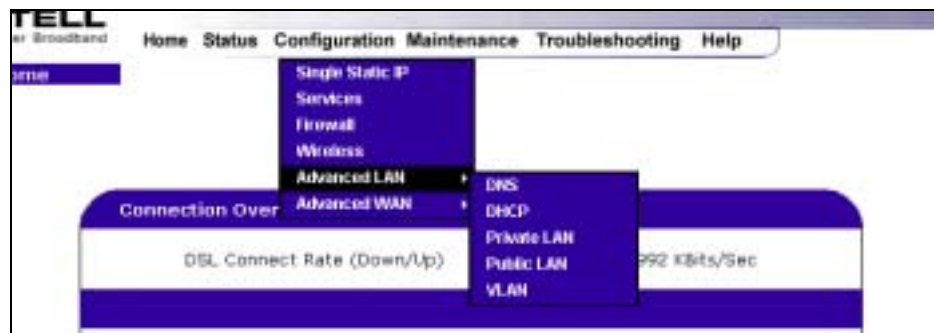


Traffic	Allowed: When the MAC Filter is enabled, only stations in the MAC Filter Table (which are set to “Allowed”) will have access to the AP. Blocked: This allows the station to remain in the table, but no access to the VersaLink is allowed.
MAC Address	The MAC address assigned to the station that you want to allow access to.
Station Name	The station name or description that the MAC address is assigned to. This is an optional field that is useful in identifying the station.

## 12.5 Advanced LAN

This section explains the configurable features of VersaLink that are available if you select **Advanced LAN** from the **Configuration** menu.

**NOTE:** If VersaLink is configured for **ETHERNET PORT 1**, **VLAN** will not be displayed. You must configure VersaLink for **DSL/ATM PORT** to access **VLAN** in the **Advanced LAN** drop-down menu. Refer to section 12.6.2.1 for details.



### 12.5.1 DNS Configuration

The following settings will be displayed if you select **DNS** from the **Advanced LAN** menu.



User Assigned DNS	
Domain Name	This field allows you to enter a Domain Name for VersaLink.
NOTE: Some ISP's may require the name for identification purposes.	To add a Domain Name, in the field under User Assigned DNS, type in your new domain name and click <b>Set</b> .
Static Host Assignment	
Host Name	This field allows you to enter a HOST name for VersaLink.
	To add a new Host name, in the field under Static Host Assignment, type in the Host Name and the IP address and click <b>Set</b> .
IP Address	Displays the IP address that is assigned to the Host Name.
Discover Local Devices	
This field displays a list of the computers on the LAN that were assigned a DHCP Address. The DNS name and IP address entry of each discovered device is displayed. (NOTE: The values in this field will be displayed barring any propagation delays. If 'No Discovered Devices' is displayed, manually refresh the screen.)	

If you want to add a new Host Name and IP address to your DNS server, enter VersaLink's **Host Name** and **IP Address** in the fields provided in the **Static Host Assignment** section.

The screenshot displays the 'DNS Configuration' web page. At the top, the Westell logo is visible. Below it, a navigation bar includes links for Home, Status, Configuration, Maintenance, Troubleshooting, and Help. The 'DNS Configuration' section is highlighted. It features three main areas: 
 

- User Assigned DNS:** A text input field for 'Domain Name' containing 'myhome.westell.com' and a blue 'Set' button.
- Static Host Assignment:** A table with two columns: 'Host Name' and 'IP Address'. It lists three existing entries: 'device0' (192.168.1.1), 'deviceweb' (192.168.1.1), and 'SmartDevice' (192.168.1.1). Each entry has a 'Set' button. Below the table are empty input fields for a new host name and IP address, followed by 'Set', 'Delete', and 'Add' buttons.
- Discovered Local Devices:** A section that currently displays 'No Discovered Devices'.

The following screen displays a **Host Name** and an **IP Address** in the fields. Now click on **add**.

WESTELL  
Router Setup Wizard

Home Status Configuration Maintenance Troubleshooting Help

**DNS Configuration**

User Assigned DNS

Domain Name: myhome.westell.com [add]

**Static Host Assignment**

Host Name	IP Address	
router	192.168.1.1	[add]
deviceweb	192.168.1.1	[delete]
SmartDevice	192.168.1.1	[delete]
devicerecovery	192.168.1.24	[add]

**Discovered Local Devices**

No Discovered Devices

If you clicked on **add**, the following screen will be displayed. The **Host Name** and **IP Address** have been added to the Static Host Assignment.

WESTELL  
Router Setup Wizard

Home Status Configuration Maintenance Troubleshooting Help

**DNS Configuration**

User Assigned DNS

Domain Name: myhome.westell.com [add]

**Static Host Assignment**

Host Name	IP Address	
router	192.168.1.1	[add]
deviceweb	192.168.1.1	[delete]
SmartDevice	192.168.1.1	[delete]
devicerecovery	192.168.1.28	[delete]
	192.168.1.28	[add]

**Discovered Local Devices**

No Discovered Devices

## 12.5.2 DHCP Configuration (Private LAN)

The following settings will be displayed if you select **DHCP** from the **Advanced LAN** menu.



DHCP Server	<p>This setting allows VersaLink to automatically assign IP addresses to local devices connected on the LAN. Westell advises setting this to enabled for the private LAN.</p> <p>Off = DHCP Server is disabled</p> <p>Private LAN = DHCP addresses will be saved into the Private LAN configuration.</p> <p>Public LAN = DHCP addresses will be saved into the Public LAN configuration. This option is only available if the Public LAN DHCP server is enabled.</p> <p>NOTE: These addresses will be overwritten if the Internet Service Provider supports dynamic setting of these values.</p>
DHCP Start Address	<p>Factory Default = 192.168.1.15</p> <p>This field displays the first IP address that the DHCP server will provide. The DHCP Start Address must be within the IP address and lower than the DHCP End Address. You may use any number from 0 to 254 in this address.</p>
DHCP End Address	<p>Factory Default = 192.168.1.47</p> <p>This field displays the last IP address that the DHCP server will provide. The DHCP End Address must be within the IP address and higher than the DHCP Start Address. You may use any number from 0 to 254 in this address.</p>

DHCP Lease Time	<p>Factory Default = 01:00:00:00</p> <p>Displays the amount of time the provided addresses will be valid, after which the DHCP client will usually re-submit a request.</p> <p>NOTE: DHCP Lease Time is displayed in the format (dd:hh:mm:ss)*. This value must be greater than 10 seconds. Seconds must be between 0 and 59, minutes must be between 0 and 59, and hours must be between 0 and 23.</p> <p>*(dd = days, hh = hours, mm = minutes, ss = seconds)</p>
-----------------	---

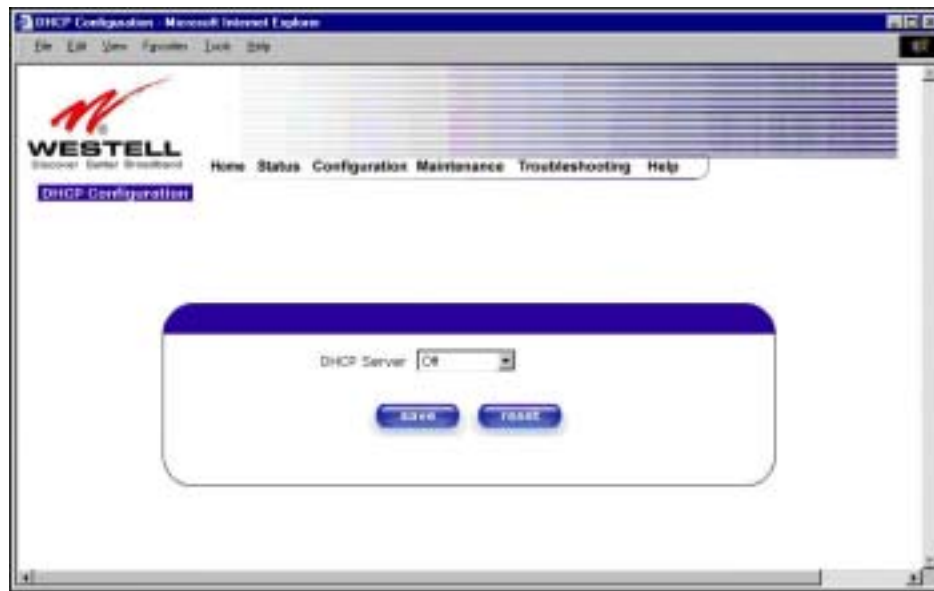
### 12.5.3 Disabling the DHCP Server

If you click on the drop-down arrow at **DHCP Server**, a list of options will be displayed.

If you want to disable your DHCP server, select **Off** from the **DHCP Server** drop-down arrow. Click on **save**.



If you selected **Off** at **DHCP Server**:, the following screen will be displayed. Click on **save** to save the **DHCP Server** setting.



If you clicked on **save**, in the preceding **DHCP Configuration** screen, the following pop-up screen will appear. Click on **OK**.



**STOP: After you disable the DHCP server, you must reboot your PC**

## 12.5.4 Enabling the DHCP Server

If you want to enable your DHCP Server settings, select **Private LAN** at the **DHCP Server** drop-down arrow.



If you have recently disabled the DHCP Server for Private LAN, select **Private LAN** while in the following screen.



If you selected **Private LAN**, the following screen will be displayed automatically. Click on **save** to save your DHCP Server setting. If you click on **reset**, your DHCP Server will be reset to factory default. (Private LAN is the factory default for the DHCP Server.)



If you clicked on **save**, the following pop-up screen will appear. Click on **OK**.



**STOP: After you enable the DHCP server, you must reboot your PC**

## 12.5.5 Private LAN Configuration – Configuring NAT

The following settings will be displayed if you select **Private LAN** from the **Advanced LAN** menu. (Private LAN is the default configuration for this VersaLink.)

NOTE: Private LAN allows you to set up a network behind VersaLink.

If you change the settings in this screen, click on **save**. If you click on **reset**, the changes will not take effect.

If you made changes and clicked on **save**, the following pop-up screen will be displayed. Click on **OK**. This will save your **Private LAN Configuration** settings. If you click **Cancel**, your new settings will not take effect.



Private LAN DHCP Server Enable	Default = CHECKED If this box is CHECKED, it enables DHCP addresses to be served from the Private LAN pool.
Private LAN Enable	Default = CHECKED

	If this box is CHECKED, it enables the addresses from the Private LAN to use the NAT interface.
Modem IP Address	Displays VersaLink's IP address
Subnet Mask	Displays the Subnet Mask, which determines what portion of an IP address is controlled by the network and which portion is controlled by the host.
DHCP Start Address	Displays the first IP address that the DHCP server will provide.
DHCP End Address	Displays the last IP address that the DHCP server will provide.
DHCP Lease Time	Displays the amount of time the provided addresses will be valid, after which the DHCP client will usually re-submit a request.

NOTE: DHCP Lease Time is displayed in the following format: (dd:hh:mm:ss)\* This value must be greater than 10 seconds. The default = 01:00:00:00. Seconds must be between 0 and 59, minutes must be between 0 and 59, and hours must be between 0 and 23.

\*(dd = days, hh = hours, mm = minutes, ss = seconds).

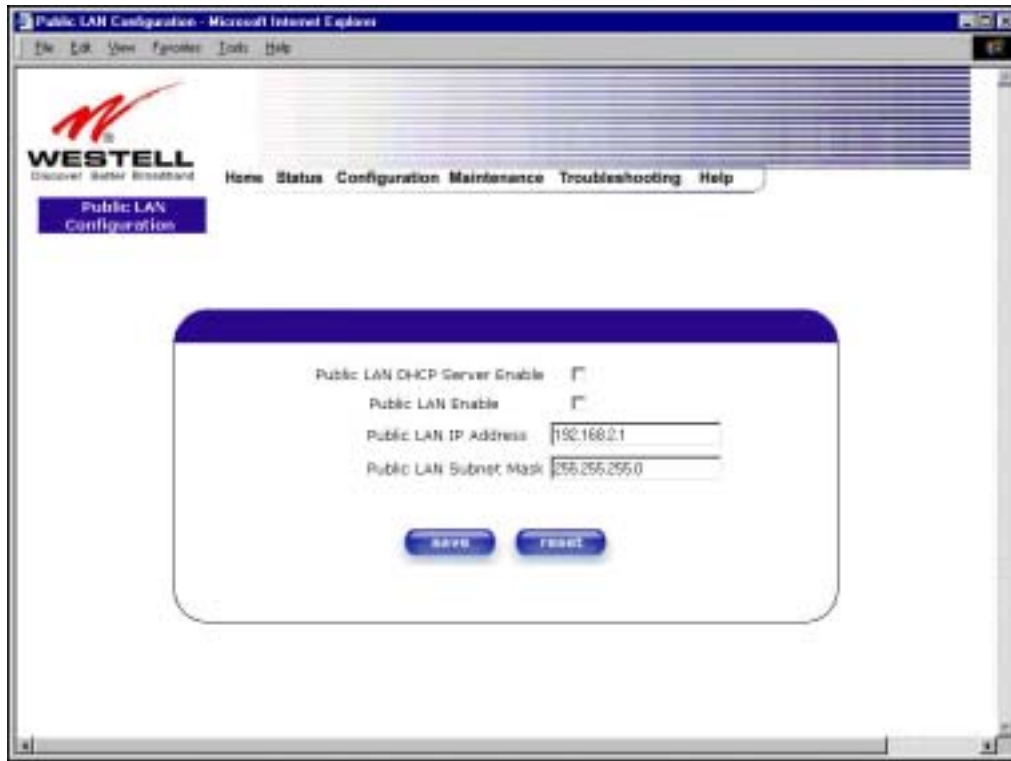
If the settings you have entered in the **Private LAN Configuration** screen are incorrect, the following warnings messages may be displayed via pop-up screens. If this occurs, check the settings in the **Private LAN Configuration** screen.

Warning Message	Check Private LAN DHCP Settings
Start Address is not part of the Subnet	Check the value in the DHCP Start Address field
End Address is not part of the Subnet	Check the value in the DHCP End Address field
End Address is below the Start Address	Check the value in the DHCP End Address field
Lease time must be greater than 10 seconds	Check the values in the DHCP Lease Time fields
Seconds must be between 0 and 59	Check the <b>Seconds</b> value in the DHCP Lease Time field
Minutes must be between 0 and 59	Check the <b>Minutes</b> value in the DHCP Lease Time field
Hours must be between 0 and 23	Check the <b>Hours</b> value in the DHCP Lease Time field

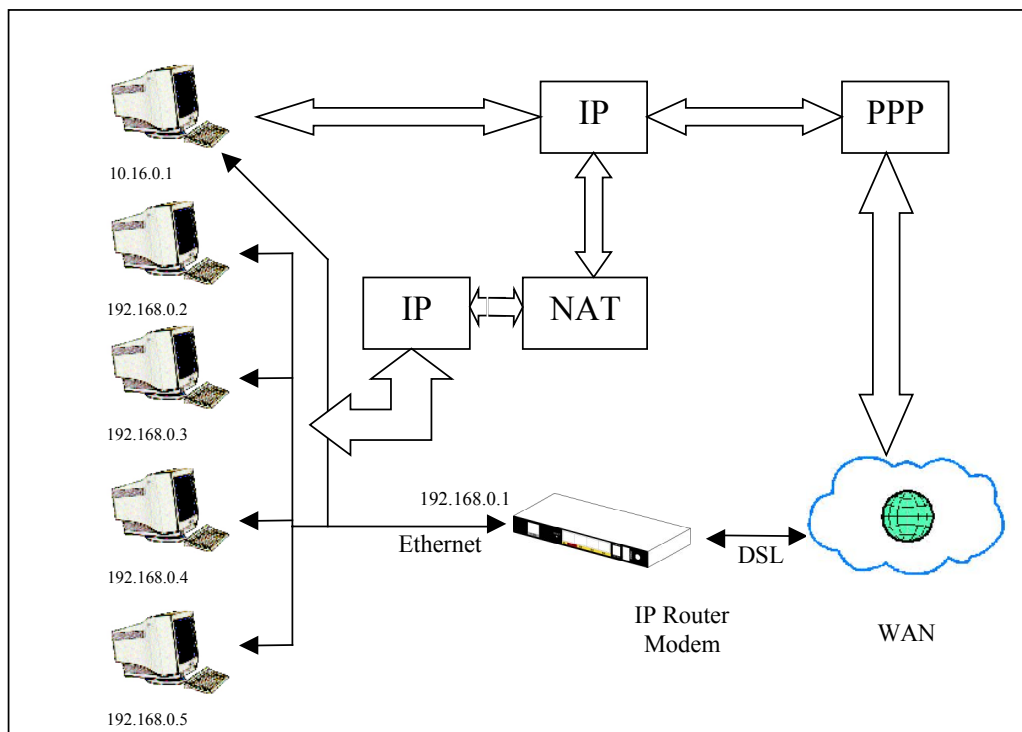
## 12.5.6 Public LAN Configuration – Multiple IP Address PassThrough

The following screen will be displayed if you select **Public LAN** from the **Advanced LAN** menu. Click in the **Public LAN DHCP Server Enable** box. A check mark will appear in the box.

NOTE: The Public LAN feature, if available from your service provider, allows VersaLink to use LAN IP addresses that are accessible from the WAN. Public LAN allows your computer to have global address ability. To utilize the Public LAN feature on VersaLink, your ISP must support Public LAN and Static IP. Contact your ISP for details.



The public devices are visible on the Internet unlike a local NAT'ed PC. The example below shows four NAT'ed PCs and one global PC. The arrows show the data path for each flow.



Public LAN DHCP Server Enable	Default = NOT CHECKED If this box is CHECKED, it enables DHCP addresses to be served from the Public LAN pool.
Public LAN Enable	Default = NOT CHECKED If this box is CHECKED, it enables the addresses from the Public LAN to bypass the NAT interface.
Public LAN IP Address	Provides a Public IP Address if the service provider does not automatically provide one.
Public LAN Subnet Mask	Provides a Public Subnet Mask if the service provider does not automatically provide one.

If you clicked on the **Public LAN DHCP Server Enable** box, the following screen will be displayed. Click on the **Public LAN Enable** box to enable Public LAN.

NOTE: By enabling the Public LAN DHCP Server, you automatically disable the Private LAN DHCP Server on VersaLink.



If you clicked on the **Public LAN Enable** box, the following screen will be displayed, showing the Public LAN Enable box selected. Click on **save**.



If you selected **Public LAN Enable**, or if you made other changes in the **Public LAN Configuration** screen and clicked on **save**, the following pop-up screen will be displayed. Click on **OK** to save the new settings. If you click on **Cancel**, your new settings will not take effect.



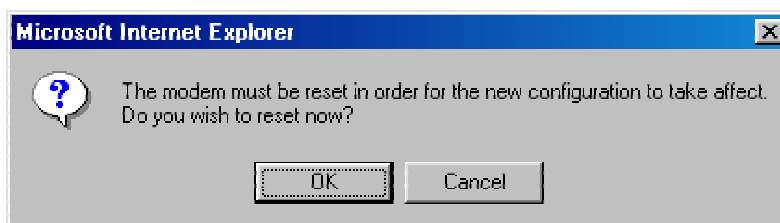
NOTE: DHCP Lease Time is displayed in the following format: (dd:hh:mm:ss)\*. This value must be greater than 10 seconds. The default = 01:00:00:00. Seconds must be between 0 and 59, minutes must be between 0 and 59, and hours must be between 0 and 23.  
\*(dd = days, hh = hours, mm = minutes, ss = seconds).

If the settings you have entered in the **Public LAN Configuration** screen are incorrect, the following warnings messages may be displayed via pop-up screens. If this occurs, check settings in the **Public LAN Configuration** screen.

Warning Message	Check Public LAN DHCP Settings
Start Address is not part of the Subnet	Check the value in the DHCP Start Address field
End Address is not part of the Subnet	Check the value in the DHCP End Address field
End Address is below the Start Address	Check the value in the DHCP End Address field

Lease time must be greater than 10 seconds	Check the values in the DHCP Lease Time fields
Seconds must be between 0 and 59	Check the <b>Seconds</b> field at DHCP Lease Time
Minutes must be between 0 and 59	Check the <b>Minutes</b> field at DHCP Lease Time
Hours must be between 0 and 23	Check the <b>Hours</b> field at DHCP Lease Time

If you clicked on **OK** in the **Load new Public LAN configuration?** screen, the following pop-up screen will be displayed. This will allow the modem to be reset and the new configuration will take effect. Click on **OK**.



If you clicked on **OK** in the preceding screen, the following screen will be displayed. VersaLink will be reset and the new configuration will take effect.



After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that your PPP session displays **UP**. (Click on the **connect** button to establish a PPP session).

**NOTE:** Whenever the PPP Status displays **DOWN**, you do not have a PPP session established. If your Gateway's connection setting is set to "Always On," after a brief delay the PPP session will be established automatically and the PPP Status will display **UP**. If the connection setting is set to "Manual," you must click on the **Connect** button to establish a PPP session. Once the PPP session has been established (PPP Status displays **UP**), you may proceed with your Gateway's configuration.

## 12.5.7 VLAN

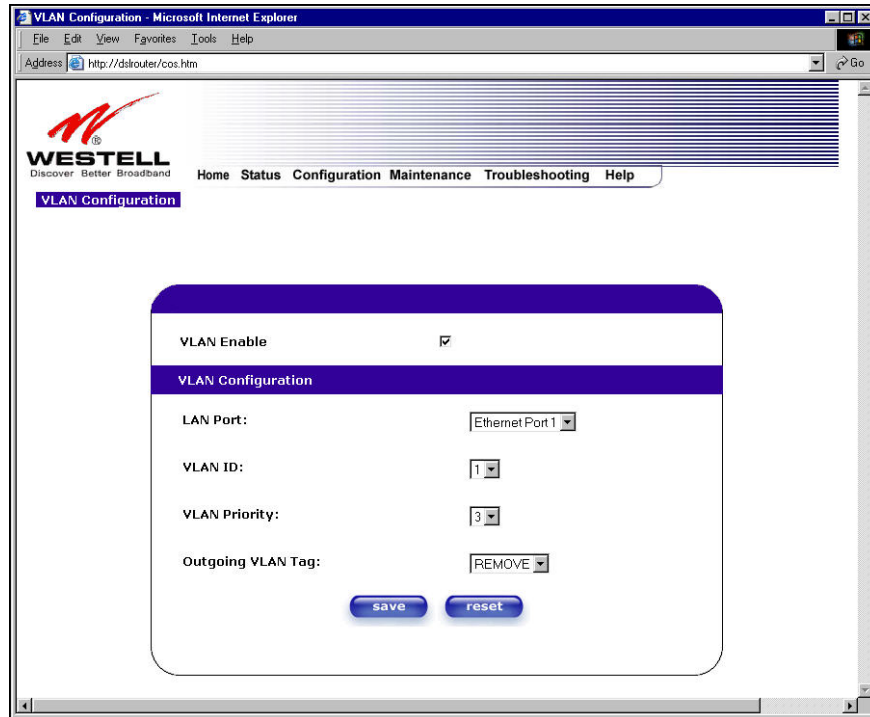
The following settings will be displayed if you select **VLAN** from the **Advanced LAN** menu.



VLAN Enable	Factory Default = DISABLED If this box is checked, VLAN will be Enabled. This will allow VLAN tagging to occur according to the data port's configuration.
LAN Port	This allows you to select the LAN port that you wish to configure. Possible responses are: Ethernet Port 1 Ethernet Port 2 Ethernet Port 3 Ethernet Port 4 WLAN Port
VLAN ID	This allows you to assign a VLAN ID to the port. Possible responses are: 1 through 8
VLAN Priority	This allows you to set the VLAN priority for the port. Possible responses are: 0 through 7
Outgoing VLAN Tag	This allows you to keep or remove the VLAN tag on the port when data is outgoing.

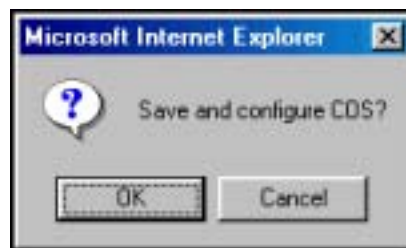
To enable VLAN click on the box adjacent to the **VLAN Enable** field. A check mark will appear in the box. Click on **save**.

**NOTE:** For VLAN to function properly, the VLAN ID must be set to a value other than '1' in **VLAN Configuration** screen and in the **VC 1 Configuration** screen when the you are using the Bridge (VLAN Bridge) protocol. See Advanced WAN section for configuring VC's (refer to section 12.6.5).



**NOTE:** If you change the values in the **VLAN Configuration** screen and click the **reset** button, the screen will display the previously set values for the LAN Port you have selected. If you change the settings in this screen, you must click **save** to save the new settings.

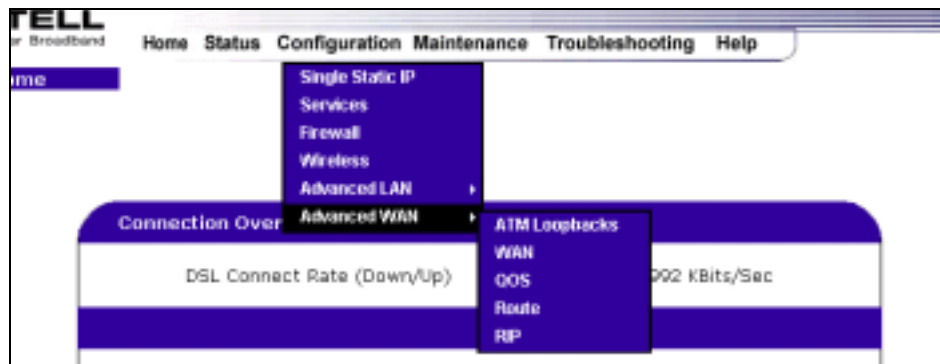
If you click on **save**, the following pop-up screen will appear. Click **OK** in the pop-up screen to allow the new settings to take effect.



## 12.6 Advanced WAN

This section explains the configurable features of VersaLink that are available if you select **Advanced WAN** from the **Configuration** menu.

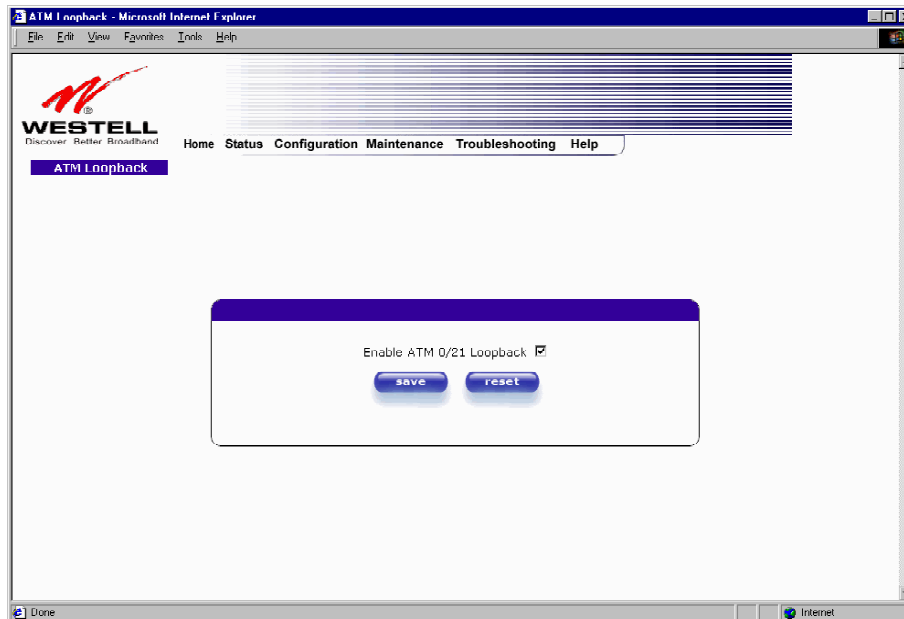
**NOTE:** If VersaLink is configured for **ETHERNET PORT 1**, **QOS** will not be displayed. You must configure VersaLink for **DSL/ATM PORT** to access **QOS** in the **Advanced WAN** drop-down menu. Refer to section 12.6.2.1 for details.



### 12.6.1 ATM Loopbacks

If you select **ATM Loopbacks** from the **Configuration** menu, the following settings will be displayed.

**NOTE:** When the **Enable ATM 0/21** box is checked, this feature is enabled. If the box does not display a check mark, this feature is disabled. If you change the setting in this screen, you must click on **save**. **Westell does not recommend that you change this setting.**

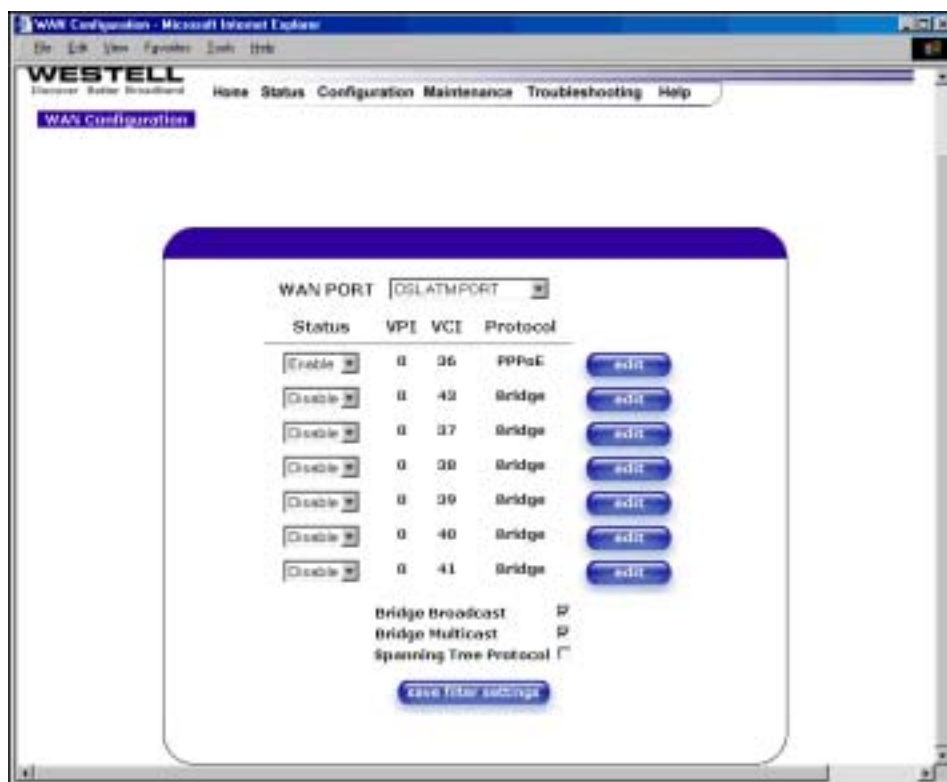


Enable ATM 0/21 Loopback:	<p>Factory Default = ENABLED</p> <p>This option enables the 0/21 loopback , which is used by your ISP. NOTE: Westell does not recommend that you change this setting.</p>
---------------------------	---

## 12.6.2 WAN Configuration

The following settings will be displayed if you select **WAN** from the **Advanced WAN** menu. If you change the **Bridge Broadcast**, **Bridge Multicast**, or **Spanning Tree Protocol** configurations in this screen, click on the **save filter settings** button to allow these changes to take effect. If you change any of the **Status** configurations, a pop-up screen will prompt you to reset the Gateway. After the Gateway has been reset, the **Status** configurations will take effect. The **edit** button allows you to change the VC configuration settings of the Gateway. Details on the **edit** button are explained later in section 12.6.3.

NOTE: The actual information displayed in this screen may vary, depending on the network connection established.



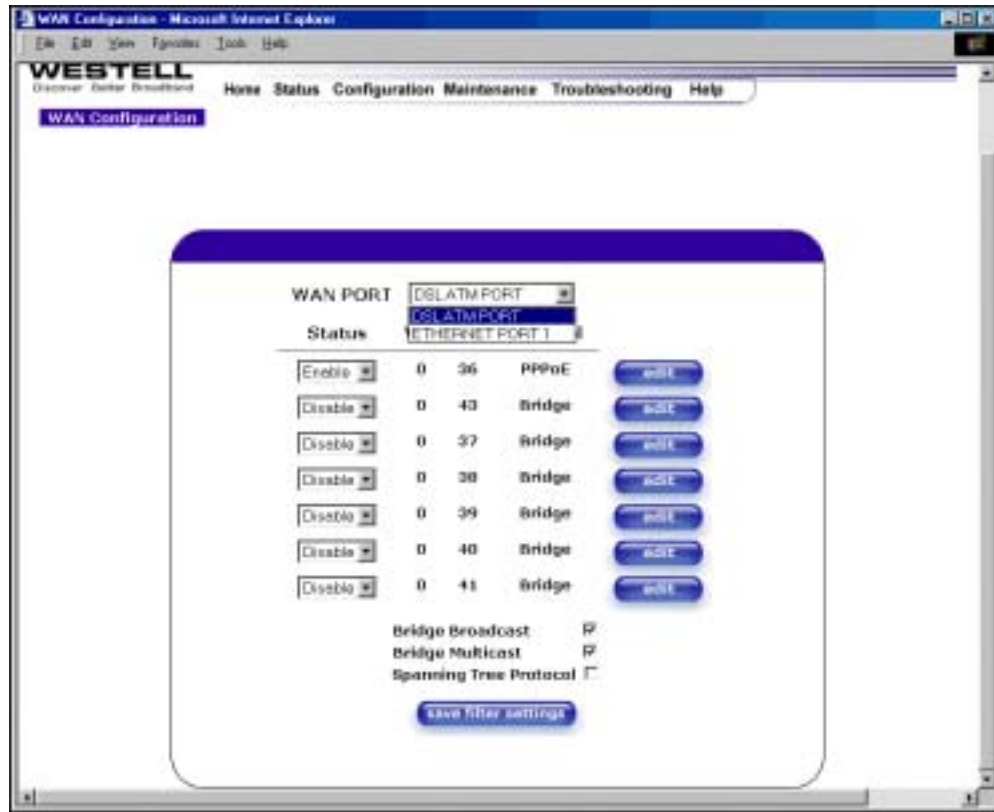
WAN PORT	Factory Default = DSL/ATM PORT Possible Responses: DSL/ATM PORT ETHERNET PORT 1
Status	Allows you to enable or disable your VC (Virtual Connection)
VPI	Displays the VPI (Virtual Path Indicator) value for a particular VC, which is defined by your Service Provider.
VCI	Displays the VCI (Virtual Channel Indicator) value for a particular VC, which is defined by your Service Provider.
Protocol	Displays the Protocol for each VC, which is specified by your Service Provider.  NOTE: The configuration specified by your Service Provider will determine which Protocols are available to you. PPPoA = Point to Point Protocol over ATM (Asynchronous Transfer Mode) PPPoE = Point to Point Protocol over Ethernet Bridge = Bridge Protocol Classical IPoA = Internet Protocol over ATM (Asynchronous Transfer Mode). This is an ATM encapsulation of the IP protocol.
Bridge Broadcast	Factory Default = CHECKED When this setting is CHECKED, VersaLink will allow Broadcast IP packets to/from the WAN. When this setting is NOT CHECKED, VersaLink will block Broadcast IP packets to/from the WAN. This setting is only valid if one of the Virtual Channels is configured for Bridge mode.
Bridge Multicast	Factory Default = CHECKED When this setting is CHECKED, VersaLink will allow Multicast IP packets to/from the WAN. When this setting is NOT CHECKED, VersaLink will block Multicast IP

	<p>packets to/from the WAN. This setting is only valid if one of the Virtual Channels is configured for Bridge mode.</p>
Spanning Tree Protocol	<p>Factory Default = DISABLED Spanning Tree Protocol is a link management protocol that provides path redundancy while preventing undesirable loops in the network. For Ethernet network to function properly, only one active path can exist between two stations.</p> <p>When ENABLED, two bridges are used to interconnect the same two computer network segments. Spanning Tree Protocol will allow the bridges to exchange information so that only one of them will handle a given message that is being sent between two computers within the network.</p> <p>NOTE: Spanning Tree can't be enabled if VLAN is enabled.</p>

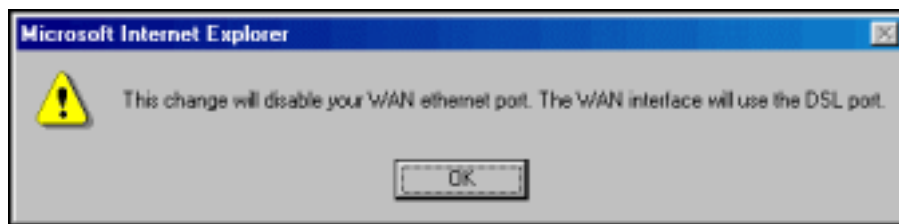
### 12.6.2.1 Enabling DSLATM PORT – Disabling ETHERNET PORT 1

To configure the VersaLink so that it uses the DSL port, select **DSLATM PORT** from the **WAN PORT** drop-down arrow. By selecting **DSLATM PORT**, you will enable the VersaLink's DSL transceiver. This will disable the WAN Ethernet port and allow the WAN interface to use the DSL port.

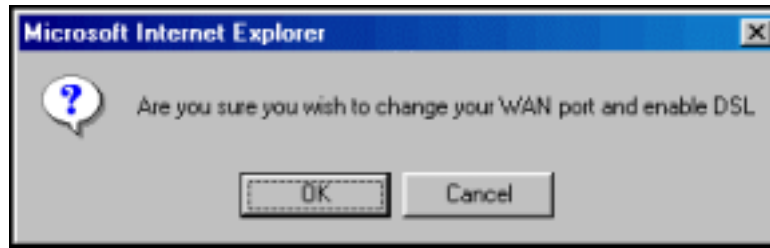
NOTE: All of VersaLink's menu options are displayed if VersaLink is configured for **DSLATM PORT**.



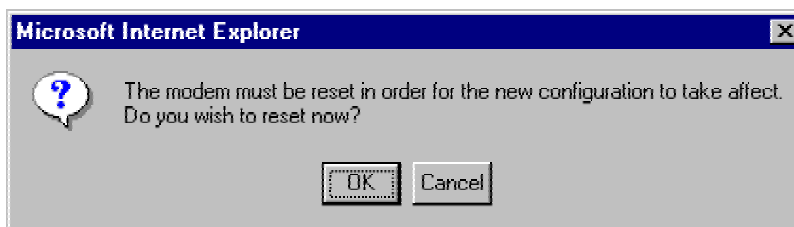
If you select **DSL/ATM PORT** from the **WAN Port** drop-down arrow, the following screen will be displayed. Click on **OK**.



If you click on **OK** in the preceding pop-up screen, the following screen will be displayed. Click on **OK**. If you click on **Cancel**, the change will not take effect.



If you clicked on **OK** in the preceding pop-up screen, the following pop-up screen will appear. VersaLink must be reset to allow the new configuration to take effect. Click on **OK**.



If you clicked on **OK** in the preceding screen, the following screen will be displayed. VersaLink will be reset and the new configuration will take effect.

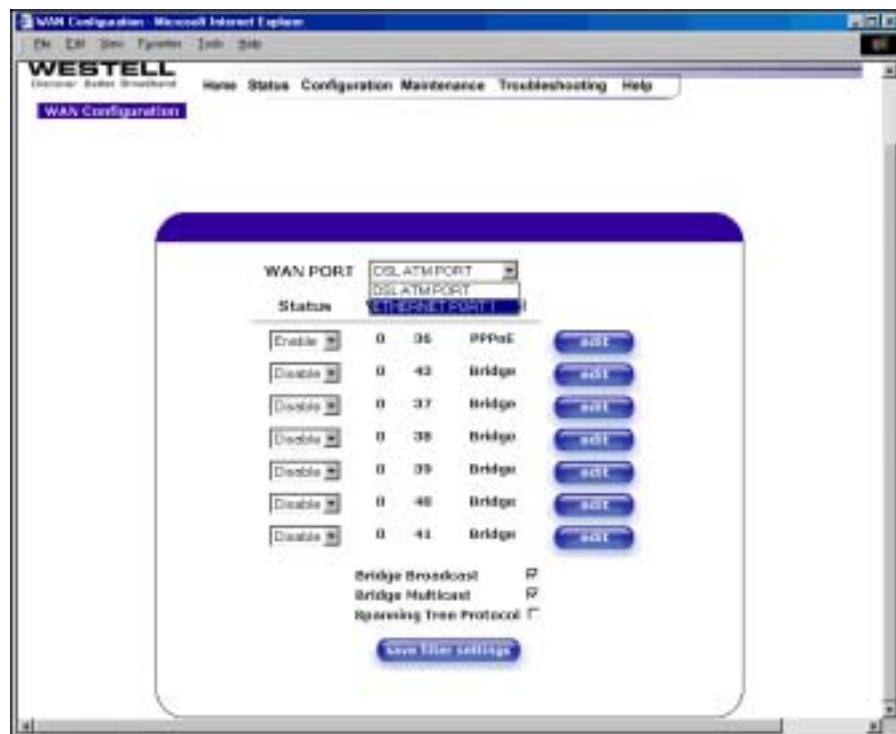


After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that your PPP session displays **UP**. (Click on the **connect** button to establish a PPP session).

## 12.6.2.2 Disabling DSLATM PORT – Enabling ETHERNET PORT 1

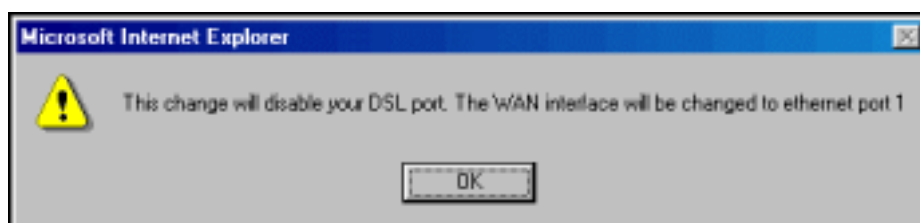
To configure the VersaLink so that it uses the WAN Ethernet Port, select **ETHERNET PORT 1** from the **WAN PORT** drop-down arrow. By selecting **ETHERNET PORT 1**, you will disable the VersaLink's DSL transceiver. This will disable the DSL Port and allow the WAN interface to use the WAN Ethernet Port.

NOTE: If ETHERNET PORT 1 is configured, the VersaLink's menu options may or may not be displayed. The sections explained throughout this document will indicate when a menu item is unavailable. The UPLINK feature is optional, and if UPLINK is not enabled in the .ini file, the Gateway will use DSL and Wireless only.

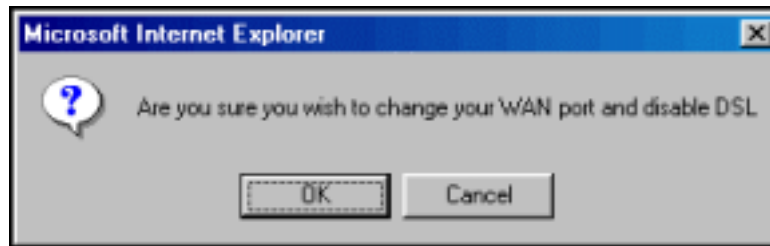


NOTE: If you experience any problems, please reset VersaLink via the external hardware reset button or via the procedure defined under the **Maintenance** menu in section 14.1. (Factory defaults become current configuration.)

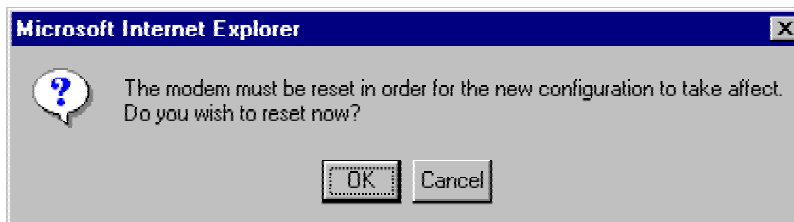
If you select **ETHERNET PORT 1** from the **WAN Port** drop-down arrow, the following screen will be displayed. Click on **OK**.



If you click on **OK** in the preceding pop-up screen, the following screen will be displayed. Click on **OK**. If you click on **Cancel**, the change will not take effect.



If you clicked on **OK** in the preceding pop-up screen, the following pop-up screen will appear. VersaLink must be reset to allow the new configuration to take effect. Click on **OK**.



If you clicked on **OK** in the preceding screen, the following screen will be displayed. VersaLink will be reset and the new configuration will take effect.



After VersaLink has been reset, the DSL LED will be OFF. This is because the DSL transceiver has now been disabled. However, the **Power**, **Ethernet**, and **Wireless** LEDs will remain lit.

### 12.6.3 Editing the WAN Configuration

The following **VC 1 Configuration** screen will be displayed if you click on the **edit** button adjacent to any of the 'Enabled' protocols displayed in the **WAN Configuration** screen. (Note: The Protocol must be enabled before you can edit its VC configuration.) The **VC 1 Configuration** screen allows you to edit your virtual connection (VC). A virtual connection identifies a connection through the service provider's ATM network to your ISP. Unlike physical hardware connections, virtual connections are defined by data.

If you change any of the VC settings in the following screen, click on the **Set VC** button.

NOTE: If you experience any problems, please reset VersaLink via the external hardware reset button or via the procedure defined under the **Maintenance** menu in section 14.1. The actual information displayed in this screen may vary, depending on network connection established.

## VC 1 Configuration

VPI   
 VCI   
 PCR   
 QoS   
 Protocol   
 Status Enabled

### VC 1 - PPPoE Settings

IP Address   
 Gateway   
 DNS Primary   
 DNS Secondary   
 MRU Negotiation ☐  
 LCP Echo Disable ☐  
 LCP Echo Failures   
*\*Must be between 1 and 30 inclusive.\**  
 LCP Echo Duration   
*\*Must be between 5 and 300 seconds inclusive and greater or equal to Retry Duration.\**  
 LCP Echo Retry Duration   
*\*Must be between 5 and 300 seconds inclusive.\**  
 Tunneling ☒ Enable ☐ Disable

Help

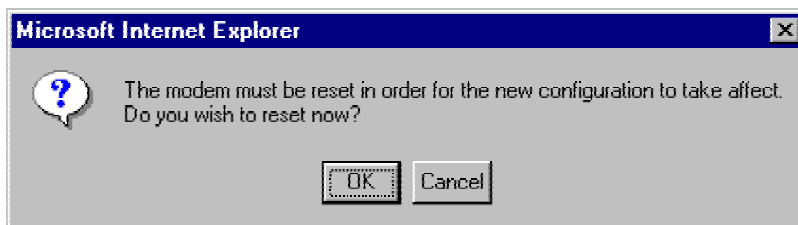
<b>VC 1 Configuration</b>	
VPI	This setting allows you to change your VPI (Virtual Path Indicator) value for a particular VC, which is defined by your Service Provider.
VCI	This setting allows you to change your VCI (Virtual Channel Indicator) value for a particular VC, which is defined by your Service Provider.
PCR	<p>Factory Default = 100%</p> <p>Peak Cell Rate (PCR)-The maximum rate at which cells can be transmitted across a virtual circuit, specified in cells per second and defined by the interval between the transmission of the last bit of one cell and the first bit of the next.</p> <p>This value is a percentage of the current data rate.  100 allows this VC to use 100% of the available bandwidth.  80 allows this VC to use 80% of the available bandwidth.</p>
QoS	<p>Quality of Service, which is determined by your Service Provider.</p> <p>Possible Responses:  CBR = Constant Bit Rate  UBR = Unspecified Bit Rate  VBR = Variable Bit Rate</p>
Protocol	<p>The Protocol for each VC, which is specified by your Service Provider.</p> <p>Possible Responses:  PPPoA = Point to Point Protocol over ATM (Asynchronous Transfer Mode)  PPPoE = Point to Point Protocol over Ethernet  Bridge = Bridge Protocol  Classical IPoA = Internet Protocol over ATM (Asynchronous Transfer Mode). This is an ATM encapsulation of the IP protocol.</p>
Status	The protocol status.
<b>VC x PPPoE Settings</b>	
IP Address	Displays the IP network address that your modem is on.
VersaLink	Displays VersaLink IP VersaLink address
DNS Primary	Provided by your Service Provider
DNS Secondary	Provided by your Service Provider
MRU Negotiation	<p>Factory Default = DISABLED</p> <p>If ENABLED, the Maximum Received Unit (MRU) would enforce MRU negotiations. (NOTE: enable this option only at your Internet Service Provider's request.)</p>
LCP Echo Disable	<p>Factory Default = Enable</p> <p>If checked, this option will disable the modem LCP Echo transmissions.</p>
LCP Echo Failures	Indicates number of continuous LCP echo non-responses received before the PPP session is terminated.
LCP Echo Retry Duration	The interval between LCP Echo transmissions with responses.
LCP Echo Retry Duration	The interval between LCP Echo after no response.
Tunneling	<p>Factory Default = ENABLE</p> <p>If ENABLED, this option allows PPP traffic to be bridged to the WAN. This feature allows you to use a PPPoE shim on the host computer to connect to the Internet Service Provider, by bypassing VersaLink's capability to do this.</p> <p>NOTE: Tunneling is available in PPPoE mode only.</p>

NOTE: The values for IP Address, VersaLink, DNS Primary, and DNS Secondary are all "Override of the value obtained from the PPP connection," They default to "0.0.0.0," in which case the override is ignored. Westell recommends that you do not change the values unless your Internet Service Provider instructs you to change them.

If you have made any changes to your VC settings, you need to save them. To save the new VC settings, click on **OK** when asked **Set this PPPoE VC configuration?** If you click on **cancel**, the new VC settings will not be saved.



If you clicked on **OK** in the preceding pop-up screen, the following pop-up screen will appear. VersaLink must be reset to allow the new configuration to take effect. Click on **OK**.



If you clicked on **OK** in the preceding screen, the following screen will be displayed. VersaLink will be reset and the new configuration will take effect.

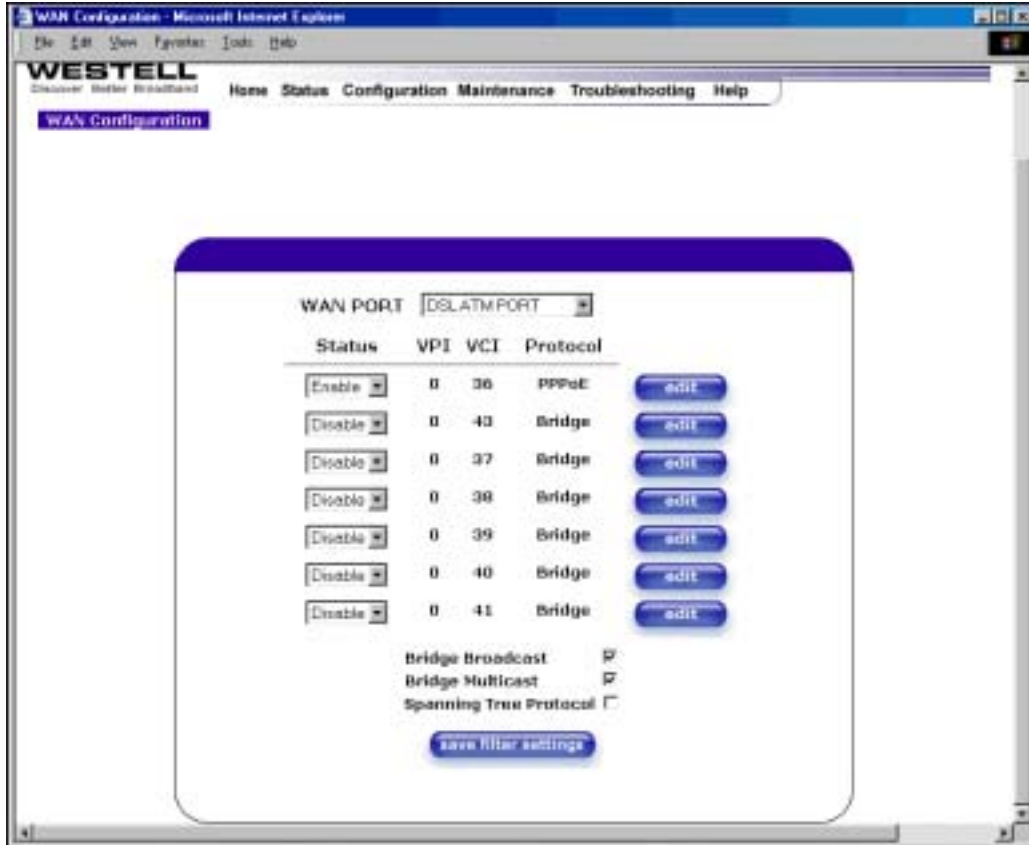


After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that your PPP session displays **UP**. (Click on the **connect** button to establish a PPP session).

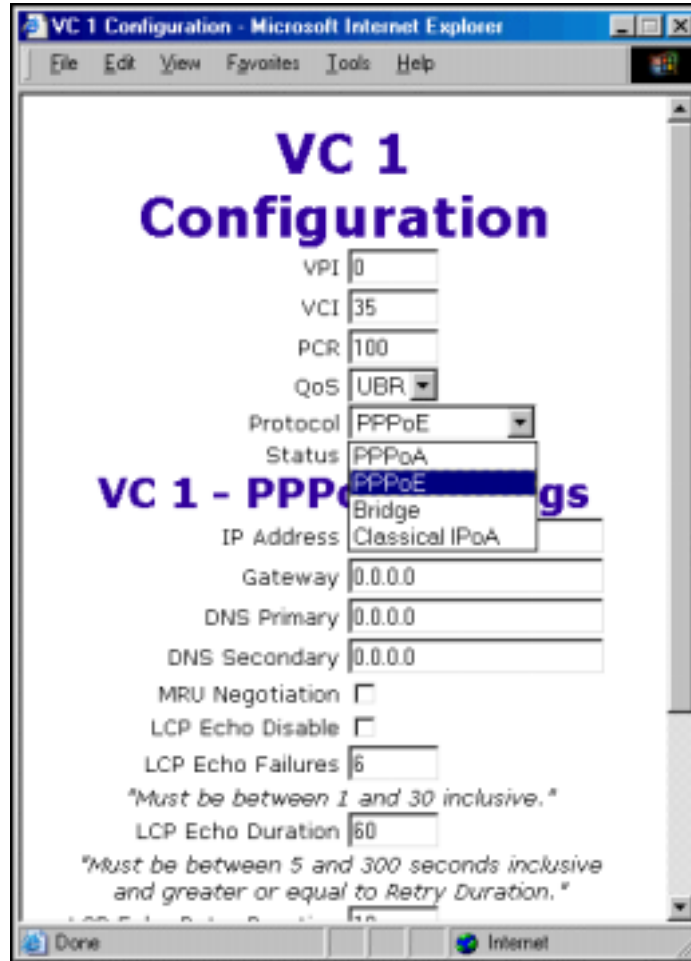
## 12.6.4 Configuring VersaLink's Protocol Settings for PPPoE Mode

To configure VersaLink's protocol settings for PPPoE mode, select **WAN** from the **Advanced WAN** menu. The **WAN Configuration** screen will be displayed. Next, click on the **edit** button adjacent to any of the existing 'Enabled' VC (Virtual Connection) protocols.

NOTE: The protocol status must display "Enable" to allow edits to its VC configuration.



If you clicked on **edit** in the **WAN Configuration** screen, the following **VC 1 Configuration** screen will be displayed. Select **PPPoE** from the options listed in **Protocol** drop-down arrow. After you have made the configuration for this protocol, select the **set VC** button.



**VC 1 Configuration**

VPI

VCI

PCR

QoS

Protocol

Status

**VC 1 - PPPoE**

IP Address

Gateway

DNS Primary

DNS Secondary

MRU Negotiation ☐

LCP Echo Disable ☐

LCP Echo Failures

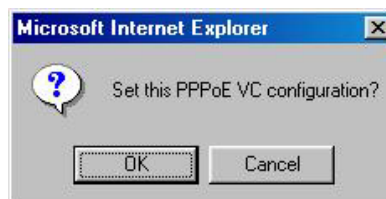
*"Must be between 1 and 30 inclusive."*

LCP Echo Duration

*"Must be between 5 and 300 seconds inclusive and greater or equal to Retry Duration."*

Done Internet

If you click the **set VC** button, the following pop-up screen will be displayed. Click on **OK** in the pop-up screen. If you click on **Cancel**, the new settings will not be saved. After you click on **OK**, follow the instructions to reset the Gateway, as previously discussed in section 12.6.3.

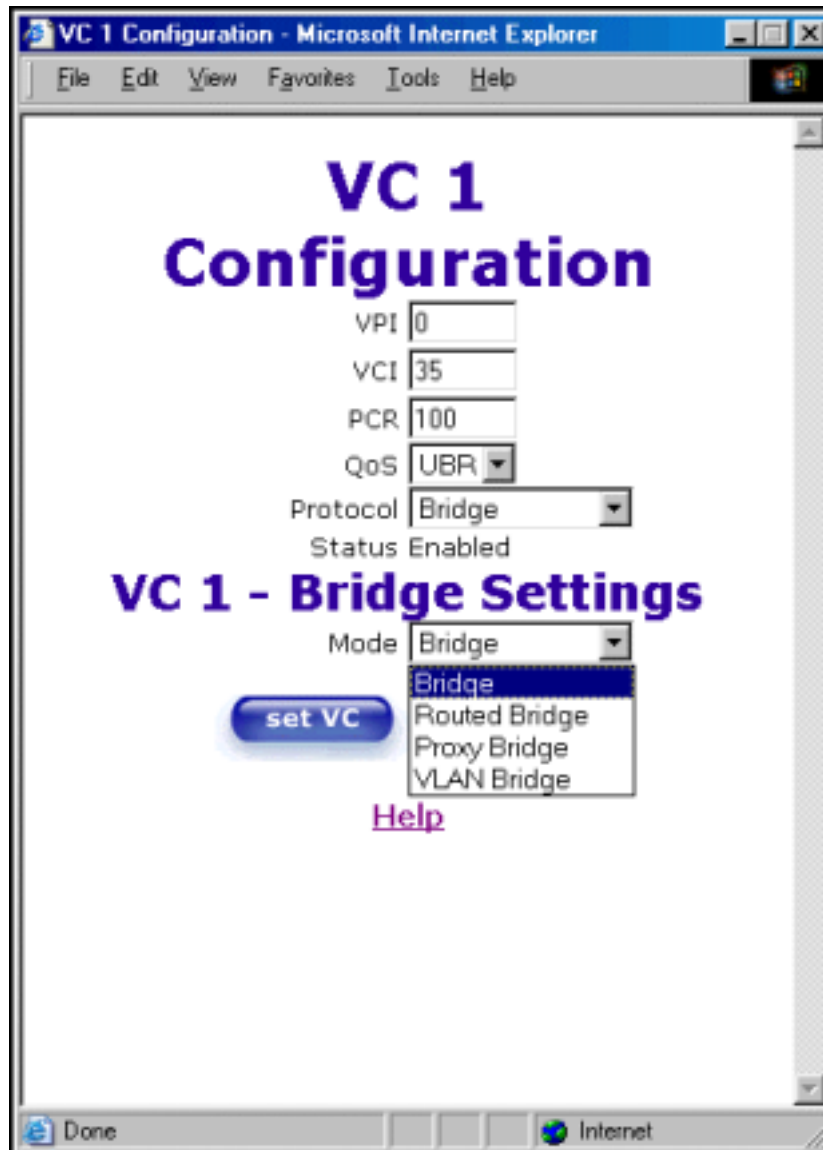


## 12.6.5 Configuring VersaLink's Protocol Settings for Bridge Mode

To configure VersaLink's protocol settings for **Bridge** mode, select **WAN** from the **Advanced WAN** menu. The **WAN Configuration** screen will be displayed. Next, click on the **edit** button adjacent to any of the existing 'Enabled' VC (Virtual Connection) protocols. The **VC1 Configuration** screen will be displayed.

NOTE: The protocol status must display "Enable" to allow edits to its VC configuration.

If you select **Bridge** protocol from the **Protocol** drop-down arrow, the following screen will be displayed. Select a mode from the options listed in the **Mode** drop-down arrow, under **VC 1 – Bridge Settings**.



**VC 1 Configuration**

VPI

VCI

PCR

QoS

Protocol

Status Enabled

**VC 1 - Bridge Settings**

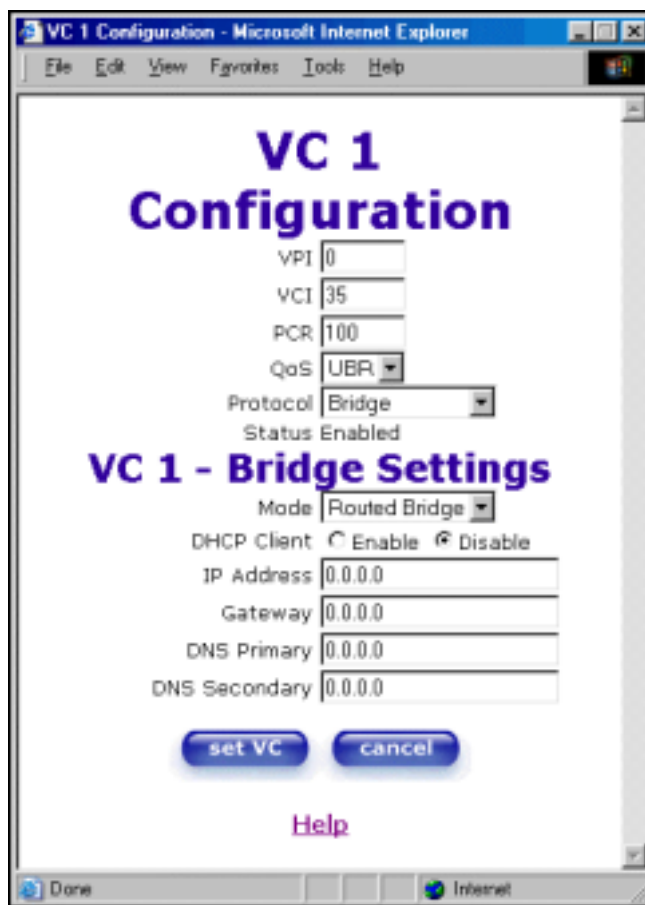
Mode

[Help](#)

Done Internet

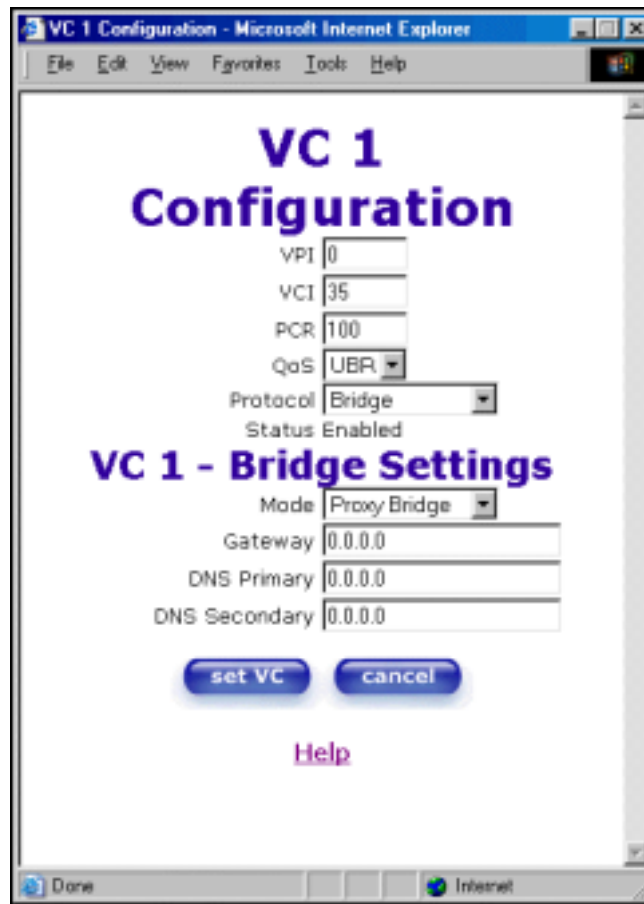
VC 1 Configuration	
VPI	This setting allows you to change your VPI (Virtual Path Indicator) value for a particular VC, which is defined by your Service Provider.
VCI	This setting allows you to change your VCI (Virtual Channel Indicator) value for a particular VC, which is defined by your Service Provider.
PCR	<p>Factory Default = 100%</p> <p>Peak Cell Rate (PCR)-The maximum rate at which cells can be transmitted across a virtual circuit, specified in cells per second and defined by the interval between the transmission of the last bit of one cell and the first bit of the next.</p> <p>This value is a percentage of the current data rate.  100 allows this VC to use 100% of the available bandwidth.  80 allows this VC to use 80% of the available bandwidth.</p>
QoS	<p>Quality of Service, which is determined by your Service Provider.</p> <p>CBR = Constant Bit Rate  UBR = Unspecified Bit Rate  VBR = Variable Bit Rate</p>
Protocol	<p>The Protocol for each VC, which is specified by your Service Provider.</p> <p>PPPoA = Point to Point Protocol over ATM (Asynchronous Transfer Mode)  PPPoE = Point to Point Protocol over Ethernet  Bridge = Bridge Protocol  Classical IPoA = Internet Protocol over ATM (Asynchronous Transfer Mode). This is an ATM encapsulation of the IP protocol.</p>
Status	The protocol status.
VC 1 Bridge Settings	
Mode	Bridge = A bridge is a layer 2 device that connects two segments of the same LAN that use the same protocol such as Ethernet. The modem does not have a WAN IP address in this mode. The client PC will typically get an IP address from a DHCP server in the network or the IP address can be assigned to the client PC statically.
	Routed Bridge = Routed Bridged Encapsulation (RBE) is the process by which a bridged segment is terminated on a routed interface. Specifically, VersaLink is routing on an IEEE 802.3 or Ethernet header carried over RFC 1483 bridged ATM. RBE was developed to address the known RFC1483 bridging issues, including broadcast storms and security. The modem will get a WAN IP address through DHCP or can be assigned statically. NAT will use the global address assigned to the modem.
	Proxy Bridge = Proxy Bridge is the process in which the modem acts as a proxy ARP agent for a local public subnet. The modem will be assigned an IP address from within that public subnet. The modem will direct all traffic to a VersaLink, which is configured statically. VersaLink address must not reside within VersaLink's assigned public subnet. All traffic will be sent via VersaLink's MAC address. The LAN may also have a private NAT'ed network. NAT will use the global address assigned to the modem.
	VLAN = Assigns VLAN tags to individual data ports on the modem.

If you selected the **Routed Bridge** mode under **VC 1- Bridge Settings**, the following screen will be displayed. Enter the appropriate values in the fields and click on **set VC**.



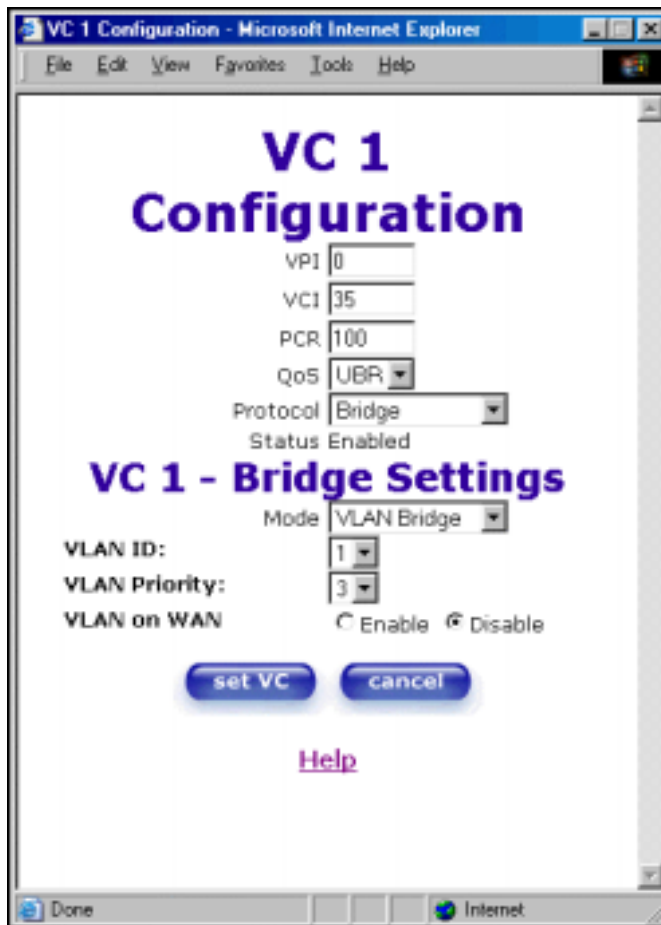
VC 1 - Bridge Settings (Routed Bridge)	
Mode	The Mode you have selected to use with Bridge protocol.
DHCP Client	Selecting a radio button allows you to either Enable or Disable the DHCP Client.
IP Address	Displays the IP network address that your modem is on.
Gateway	Displays the modem's IP gateway address.
DNS Primary	Provided by your Service Provider.
DNS Secondary	Provided by your Service Provider.

If you selected **Proxy Bridge** mode under **VC 1- Bridge Settings**, the following screen will be displayed. Enter the appropriate values in the fields and click on **set VC**.



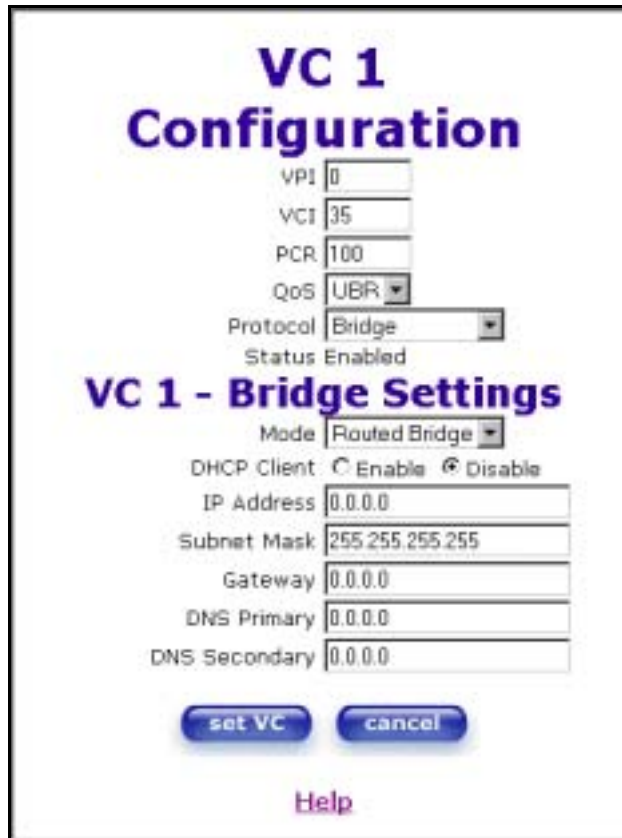
VC 1 - Bridge Settings (Proxy Bridge)	
Mode	The Mode you have selected to use with Bridge protocol.
Gateway	Displays the modem's IP address.
DNS Primary	Provided by your Service Provider.
DNS Secondary	Provided by your Service Provider.

If you selected **VLAN Bridge** under **VC 1- Bridge Settings**, the following screen will be displayed. Enter the appropriate values in the fields and click on **set VC**.



VC 1 - Bridge Settings (VLAN Bridge)	
Mode	The Mode you have selected to use with Bridge protocol. VLAN is used to assign VLAN tags to individual data ports on the modem.
VLAN ID	Assigns a VLAN ID to the port.
VLAN Priority	This will set the VLAN priority for the port.
VLAN on WAN	Factory Default = DISABLE Selecting Enable allows VLAN tagging to occur according to the data port's configuration.

After you have configured the VC 1 Configuration screen, you must click the **set VC** button to save your VC settings.



**VC 1 Configuration**

VPI

VCI

PCR

QoS

Protocol

Status Enabled

**VC 1 - Bridge Settings**

Mode

DHCP Client ☐ Enable ☒ Disable

IP Address

Subnet Mask

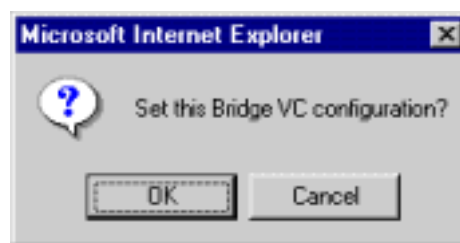
Gateway

DNS Primary

DNS Secondary

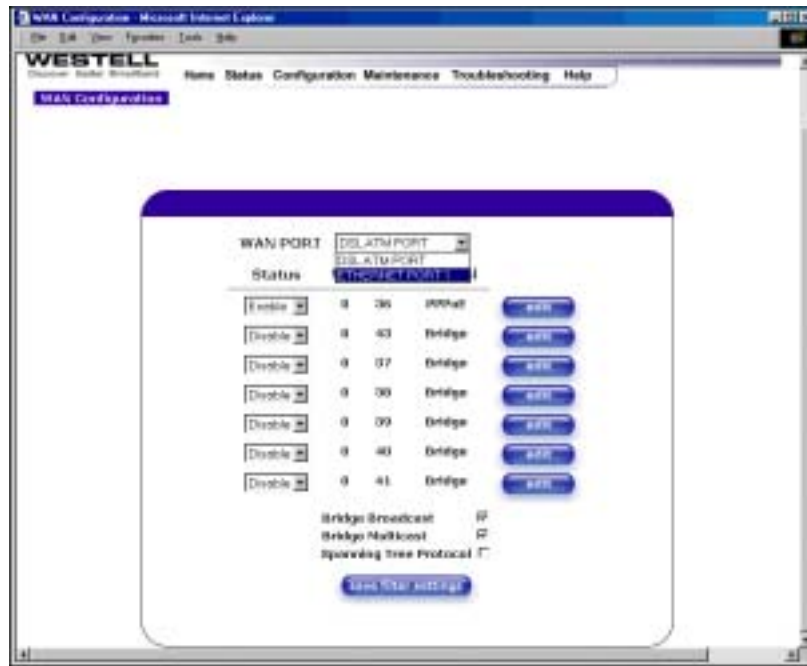
[Help](#)

If you click the **set VC** button, the following pop-up screen will be displayed. Click on **OK** in the pop-up screen. If you click on **Cancel**, the new settings will not be saved. After you click on **OK**, follow the instructions to reset the Gateway, as previously discussed in section 12.6.3.

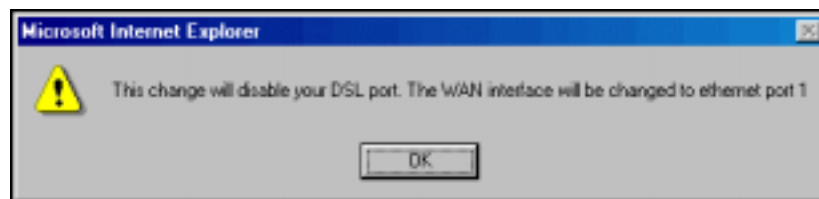


## 12.6.6 Configuring VC Protocol Settings for ETHERNET PORT 1

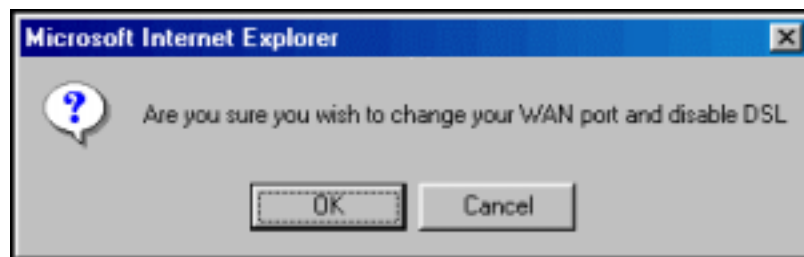
To configure the Gateway's VC settings via the Ethernet uplink port, select **ETHERNET PORT 1** at the **WAN Port** drop-down arrow.



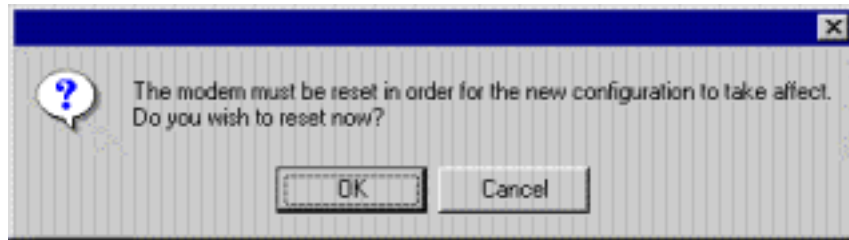
If you select **ETHERNET PORT 1**, the following pop-up will be displayed. Click on **OK**.



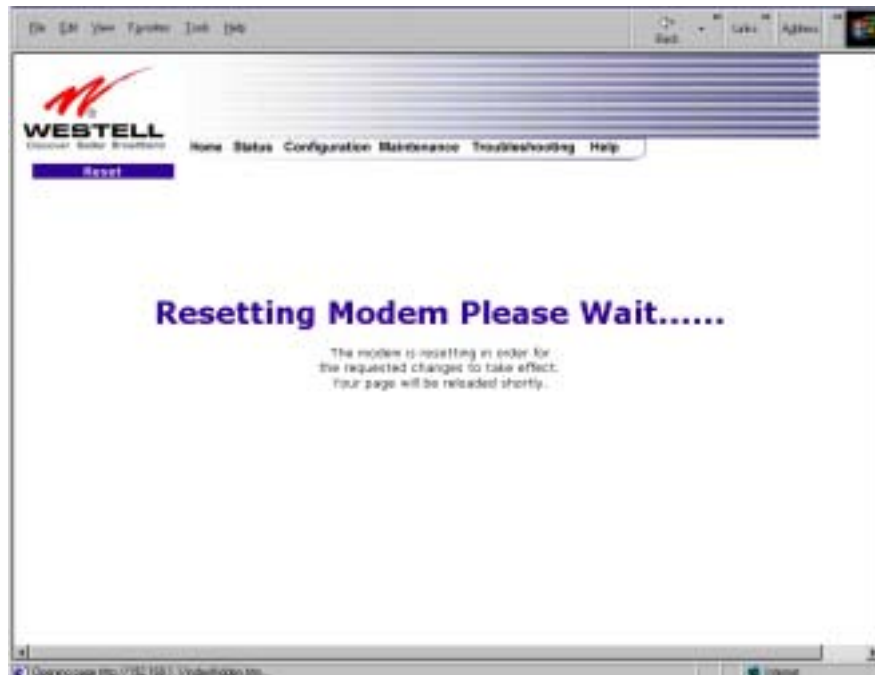
If you click on **OK**, the following pop-up screen will be displayed. Click on **OK**.



If you click on **OK** in the preceding pop-up screen, the following pop-up screen will be displayed. Click on **OK**.



If you clicked on **OK**, the following screen will be displayed. VersaLink™ will be reset and the new configuration will take effect.



After the Gateway has been reset, from the **Configuration** menu, select **Advanced WAN** and then select **WAN**. The following screen will be displayed



If you click **edit**, the following screen will be displayed. By using this screen, you can configure the WAN Ethernet port settings of your Gateway.

## WAN Ethernet Configuration

Protocol PPPoE  
Status Enabled

### PPPoE Settings

IP Address 0.0.0.0

Gateway 0.0.0.0

DNS Primary 0.0.0.0

DNS Secondary 0.0.0.0

Subnet Mask  

MRU Negotiation ☐

LCP Echo Disable ☐

LCP Echo Failures 6  
\*Must be between 1 and 30 inclusive.\*

LCP Echo Duration 60  
\*Must be between 5 and 300 seconds inclusive and greater or equal to Retry Duration.\*

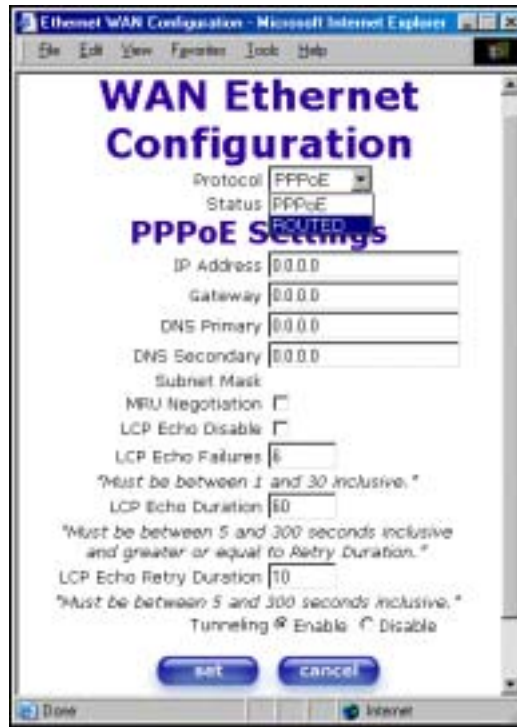
LCP Echo Retry Duration 10  
\*Must be between 5 and 300 seconds inclusive.\*

Tunneling ☒ Enable ☐ Disable

set
cancel

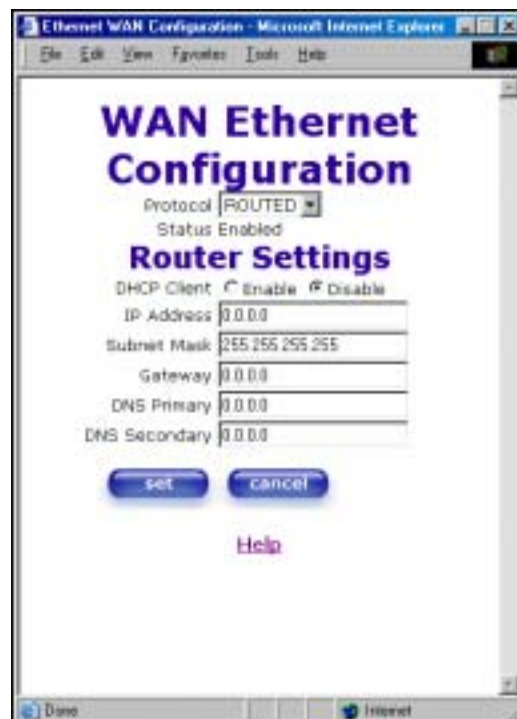
[Help](#)

To configure the WAN Ethernet port for routed bridge protocol, select **ROUTED** from the **Protocol** drop-down arrow.



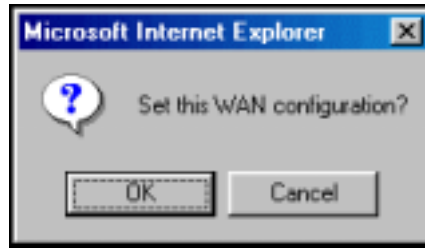
The screenshot shows the 'WAN Ethernet Configuration' window in Microsoft Internet Explorer. The 'Protocol' dropdown is set to 'PPPoE'. Below it, the 'Status' is 'PPPoE'. The 'PPPoE Settings' section includes fields for IP Address, Gateway, DNS Primary, and DNS Secondary, all set to 0.0.0.0. There are checkboxes for MRU Negotiation and LCP Echo Disable, both unchecked. The LCP Echo Failures field is set to 6, with a note: '\*Must be between 1 and 30 inclusive.\*'. The LCP Echo Duration field is set to 60, with a note: '\*Must be between 5 and 300 seconds inclusive and greater or equal to Retry Duration.\*'. The LCP Echo Retry Duration field is set to 10, with a note: '\*Must be between 5 and 300 seconds inclusive.\*'. The Tunneling option is set to 'Enable'. At the bottom are 'set' and 'cancel' buttons.

If you select **ROUTED**, the following screen will be displayed. Enter the appropriate values in the fields and click on **set**.

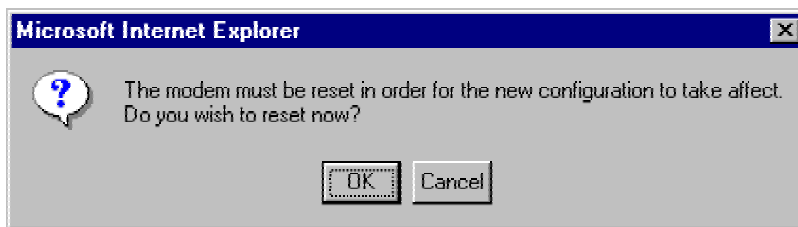


The screenshot shows the 'WAN Ethernet Configuration' window in Microsoft Internet Explorer. The 'Protocol' dropdown is set to 'ROUTED'. Below it, the 'Status' is 'Enabled'. The 'Router Settings' section includes a 'DHCP Client' checkbox set to 'Disable'. The IP Address field is set to 0.0.0.0, the Subnet Mask field is set to 255.255.255.255, the Gateway field is set to 0.0.0.0, the DNS Primary field is set to 0.0.0.0, and the DNS Secondary field is set to 0.0.0.0. At the bottom are 'set' and 'cancel' buttons, and a 'Help' link.

If you click on **set**, the following pop-up screen will be displayed. Click on **OK**.



If you clicked on **OK** in the preceding pop-up screen, the following pop-up screen will appear. VersaLink must be reset to allow the new configuration to take effect. Click on **OK**.



If you clicked on **OK** in the preceding screen, the following screen will be displayed. VersaLink will be reset and the new configuration will take effect.



After the modem has been reset, the **WAN Configuration** screen will display **Routed Bridge** as the protocol for **ETHERNET PORT 1**.



## 12.6.7 QOS

The following settings will be displayed if you select **QOS** from the **Advanced WAN** menu. If you change any settings in this screen, click on **save**. If you click on **reset**, this screen will refresh and display your last saved QoS configuration.

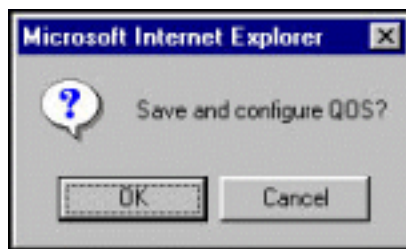
NOTE: The QOS feature helps ensure data integrity in high-speed transmissions. QOS provides the capability to partition network traffic into multiple priority levels or classes of service. After packet classification, other QOS features can be utilized to assign the appropriate traffic handling policies including congestion management, bandwidth allocation, and delay bounds for each traffic class.



QOS Enable	Factory Default = DISABLED If this box is checked, Quality of Service (QOS) will be Enabled.
Turbo TCP Enable	Factory Default = DISABLED If this box is checked, Turbo TCP will be Enabled.
QOS Configuration	
QOS Filter Enable	Factory Default = DISABLED If this box is checked, this will Enable the QOS filter.
QOS Classification	This feature provides the capability to partition network traffic into multiple priority levels or classes of service. After packet classification, other QoS features can be utilized to assign the appropriate traffic handling policies including congestion management, bandwidth allocation, and delay bounds for each traffic class.

	Possible responses are: Best Effort (BE) Assured Forwarding (AF1) Assured Forwarding (AF2) Assured Forwarding (AF3) Assured Forwarding (AF4) Expedited Forwarding (EF) Network Control (NC)
Peak Information Rte (%)	The maximum allowed rate for this priority, expressed as a percentage of the DSL rate.
Committed Information Rate (%)	The committed rate for this priority, expressed as a percentage of the DSL rate.
Peak Burst Size	The interval in milliseconds for averaging the peak offered rate.
Committed Burst Size	The interval in milliseconds for averaging the committed offered rate.
Max Queue Size	The number of packets that can be queued for this priority.
Latency Measurements	
Latency Boundary	This configures the maximum latency boundary in milliseconds that a specific packet may be delayed by.
Latency Threshold (ms)	This setting configures the maximum latency boundary in milliseconds that a specific packet may be delayed by. Possible responses are: Boundary 1:0 ms Boundary 2:10 ms Boundary 3:30 ms Boundary 4:40 ms Boundary 5:100 ms Boundary 6:1000 ms Boundary 7:3000 ms
IP Fragmentation Enable	Factory Default = DISABLED If this box is checked, IP Fragmentation will be Enabled. If Enabled and packets larger than 1500 bytes total are received, they will be fragmented.
IP Fragment Size	This is the IP Packet Size. Possible responses are: 100, 148, 244, 292, 340, 388, or 436

If you made changes to the **QOS Configuration** and clicked on **save**, the following screen will be displayed. Click on **OK**. This will save your new QOS settings.



## 12.6.8 Route

The following settings will be displayed if you select **Route** from the **Advanced WAN** menu. The Route table maintains the routes or paths of where specific types of data shall be routed across a network.

*Note: In this screen, VersaLink represents 'Gateway.'*

To add a Route, enter a **Subnet Mask** address, or check the **Host Route** box. Click on the **add** button to establish a static route.

IP Interfaces	
IP Interfaces	The list of active interfaces on the modem and their IP and Subnet mask address. Eth0 is the local LAN interface. Lo0 is the loopback interface.
Address	The IP interface address.
Subnet Mask	The IP interface subnet address.
Name	The IP interface device name.
Network Routing Table	
Network Routing Table	The list of network routes. These can be either routes for directly connected interfaces or static routes.
Destination Address	The IP address or subnet of the Route.
Subnet Mask	If the Route is a network route, Subnet Mask is used to specify the subnet address. If the Route is a Host route, then the Host Route check box is used.
VersaLink	Indicates where to send the packet if it matches this route.

Interface	Indicates where to send the packet if it matches this route.
Metric	The RIP metric to be assigned to this route if and when it is advertised using RIP.
RIP	Indicates whether a static route should be advertised via RIP.
<b>Host Routing Table</b>	
Host Routing Table	The list of host routes. A host route is an IP route with a 32-bit mask, indicating a single destination (as opposed to a subnet, which could match several destinations.)
Destination Address	The IP address or subnet of the Route.
Subnet Mask	If the Route is a network route, Subnet Mask is used to specify the subnet address. If the Route is a Host route, then the Host Route check box is used.
VersaLink	Indicates where to send the packet if it matches this route.
Interface	Indicates where to send the packet if it matches this route.
Metric	The RIP metric to be assigned to this route if and when it is advertised using RIP.
RIP	Indicates whether a static route should be advertised via RIP.
<b>Inactive Routes</b>	
Inactive Routes	Static routes whose interface is currently not in service.
Destination Address	The IP address or subnet of the Route.
Subnet Mask	If the Route is a network route, Subnet Mask is used to specify the subnet address. If the Route is a Host route, then the Host Route check box is used.
VersaLink	Indicates where to send the packet if it matches this route.
Interface	Indicates where to send the packet if it matches this route.
Metric	The RIP metric to be assigned to this route if and when it is advertised using RIP.
RIP	Indicates whether a static route should be advertised via RIP.
<b>Add Route</b>	
Add Route	This is used to add a new static route in the modem.
Destination Address	The IP address or subnet of the Route.
Subnet Mask/ Host Route	If the Route is a network route, Subnet Mask is used to specify the subnet address. If the Route is a Host route, then the Host Route check box is used.
VersaLink/IP Address	The interface to use for sending the packet, if it matches this route. (Only active VersaLinks can be used to create a static route.)
Metric	The RIP metric to be assigned to this route if and when it is advertised using RIP.
RIP Conf	Determines whether or not to advertise the static route, using RIP. (RIP must also be enabled before the route will be advertised.)
Save to Modem	If checked, then the route will be made permanent by saving it to flash memory. If not checked, the route will disappear the next time the modem restarts.

## 12.6.9 RIP

The following details will be displayed if you select **RIP** from the **Advanced WAN** menu. If you change any settings in this screen, click on **save**. If you click on **reset**, this screen will refresh and display your last saved RIP configuration.

RIP (Routing Interface Protocol) is a dynamic inter-network routing protocol primarily used in interior routing environments. A dynamic routing protocol, as opposed to a static routing protocol, automatically discovers routes and builds routing tables.

The screenshot shows the Westell VersaLink Gateway web interface for RIP configuration. At the top, there's a navigation bar with links: Home, Status, Configuration, Maintenance, Troubleshooting, and Help. Below this is a 'RIP Configuration' tab. The main content area is divided into three sections: 'RIP Enable' with a checkbox, 'RIP Configuration' with four dropdown menus (Interface Type: LAN, Receive: RIPv2, Transmit: RIPv2, RIPv2 Authentication Mode: None), and 'Advanced' with several settings: Default Gateway (checkbox), Border Gateway Filtering (checkbox), RIP Timer Rate (input field), RIP Supply Interval (input field), RIP Expire Time (input field), and RIP Garbage Collection Time (input field). At the bottom of the configuration area are 'Save' and 'Reset' buttons.

*Note: In this screen, Versa Link represents 'Gateway.'*

RIP Enable	Factory Default = DISABLED If this box is checked, RIP will be Enabled (turned ON).
RIP Configuration	
Interface Type	LAN: Select this if you are configuring RIP for the LAN side. WAN: Select this if you are configuring RIP for the WAN side. (WAN side is receive only.)
Receive	The version of RIP to be accepted. Possible responses are: None RIPv1 RIPv2

	RIPv1 or RIPv2
Transmit	The version of RIP to be transmitted. (WAN side RIP never transmits) Possible responses are: None RIPv1 RIPv1 Compatible RIPv2
RIPv2 Authentication Mode	If using RIP V2, you must select the type of authentication to use. Possible responses are: None Clear Text MD5 (If MD5 authentication, the password)
Advanced	
Default VersaLink	Factory Default = DISABLED If this box is check (Enabled), this feature will determine whether the modem advertises itself as a VersaLink (i.e., the default route)
Border VersaLink Filtering	Factory Default = ENABLED If this box is unchecked (Disabled), the modem will not summarize subnets into a single route before advertising.
RIP Timer Rate	Indicates how often to update the local routing table.
RIP Supply Interval	Indicates how often to advertise routes to neighbors.
RIP Expire Time	Indicates how long routes received from neighbors become invalid, if no refresh of the route is received.
RIP Garbage Collection Time	Indicates how long to advertise invalid routes after they have expired.

If you change any settings in the **RIP Configuration** screen and clicke on **save**, the following screen will be displayed. Click on **OK** to save your new RIP settings.

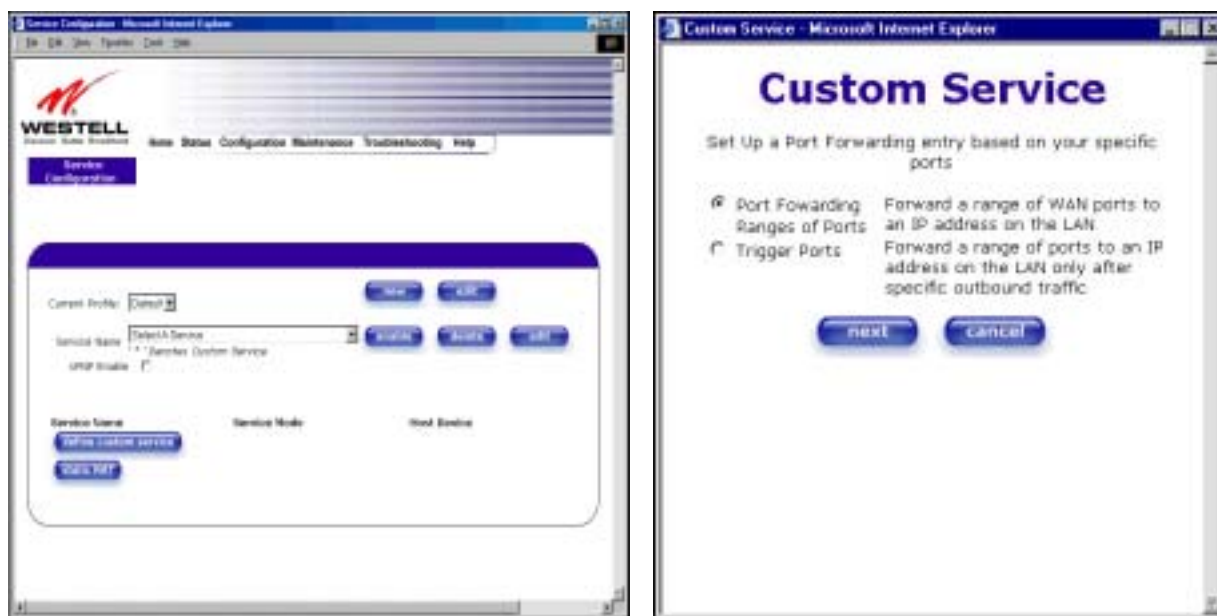


## 13. SETTING UP ADVANCED SERVICE CONFIGURATION

You can set up additional Service Configuration options for VersaLink that allow you to enter the port forwarding and trigger ports ranges of your choice. Go to **Configuration** at the homepage menu and select **Services**.

When you click on **define custom service** in the **Service Configuration** screen, the **Custom Service** screen will guide you through the steps of creating an advanced NAT service entry via the **define custom service** button.

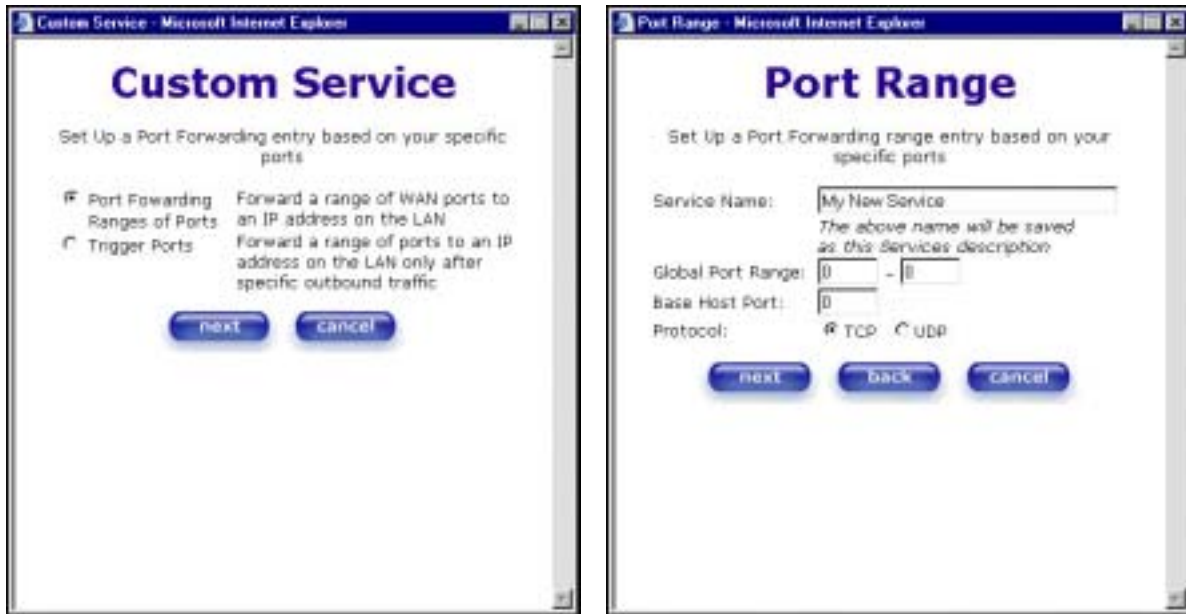
**NOTE:** Westell strongly recommends that you do not change any values in this section. If you experience any problems, please reset VersaLink via the external hardware reset button or the procedure defined under the **Maintenance** menu.



Port Forwarding Ranges of Ports	This option allows you to forward a range of WAN ports to an IP address on the LAN.
Trigger Ports	This option allows you to forward a range of ports to an IP address on the LAN only after specific outbound traffic.


## 13.1 Port Forwarding Ranges of Ports

To select **Port Forwarding Ranges of Ports**, click on **define custom service** from the **Service Configuration** screen, and then select **Port Forwarding Ranges of Ports** from the **Custom Service** screen. Click on **Next**. The **Port Range** screen will be displayed. Enter your values in the **Global Port Range** fields and click **next** to continue.



## 13.2 Adding Port Forwarding Ports

If you made changes in the **Port Range** screen and clicked on **next**, the following screen will be displayed. Click on **close** to accept the changes, or click on **add** to go back to **Port Range** screen and enter additional port range values. You can repeat this step for each range of ports that you want to add (up to 62 port forwarding ranges). When you are finished adding ports to the Global Port Range, you must click on **close** to accept the information you have entered and return to the **Service Configuration** screen.



Service Name	The NAT service for which you are configuring Port Forwarding.
Type	The type of NAT service configuration you selected.
Protocol	The type of Protocol that is used to run this NAT service. TCP- Transmission Control Protocol. UDP-User Datagram Protocol (UDP).
Local IP Address	If a static IP address has been assigned, it will be displayed here.
Base Host Port	The port on the WAN that will host the NAT service selected. Base Host Port is the first port that will be used for a specific service when configured for a range of ports.

### 13.3 Port Forwarding Trigger Ports

To select **Port Forwarding Trigger Ports**, click on **define custom service** from the **Service Configuration** screen, and then select **Trigger Ports** from the **Custom Service** screen. Click on **next**. The follow settings will be displayed in the **Trigger Ports** screen. Enter your values in the **Local 'Trigger' Port Range** fields and click on **next** to continue.




Service Name	The NAT service you selected.
Local Trigger Port Range	The local LAN side TCP/UDP port.
Global Port Range	The WAN side TCP/UDP port range.

## 13.4 Adding Local Trigger Ports

If you made changes in the **Local ‘Trigger’ Port Range** screen and clicked **next**, the following screen will be displayed. Click on **close** to accept the changes, or click on **add** to go back to the **Trigger Ports** screen and enter additional port range values. You can repeat this step for each port range that you want to add (up to 10 trigger ports). When you are finished adding ports to the Local ‘Trigger’ Port Range, you must click on **close** to accept the information you have entered and to return to the **Service Configuration** screen.

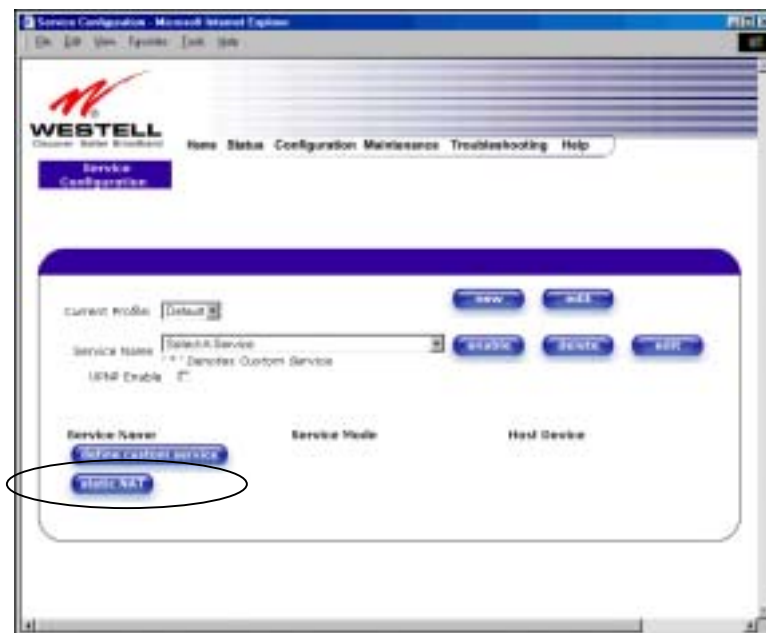


## 13.5 Static NAT

If you select **Services** from the **Configuration** menu, the following screen will be displayed, showing the static NAT button. Static NAT allows you to configure VersaLink to work with the special NAT services.

**NOTE:** When the Gateway is configured for Static NAT, any unsolicited packets arriving at the WAN would be forwarded to this device. This feature is used in cases where the user wants to host a server for a specific application.

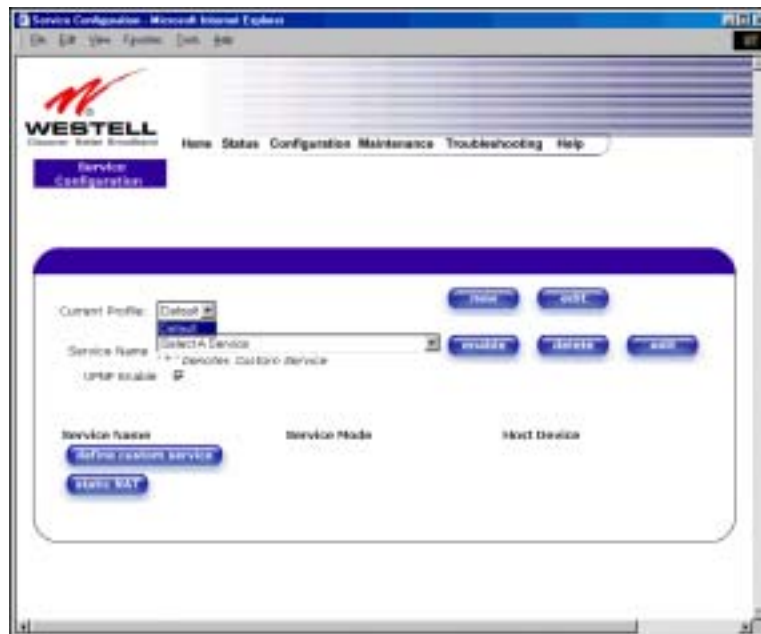
**STOP:** Single Static IP must be disabled (if it has been enabled previously) before you enable **static NAT**. To disable Single Static IP, select **Single Static IP** from the **Configuration** menu. Next, click on the **disable** button, and then click on **OK** in the pop-up screens to allow the Gateway to be reset. As explained in section 12.1 (Single Static IP), you must reboot your computer after you enable or disable Single Static IP. After you have rebooted your computer, return to static NAT configuration screen by selecting **Services** from the **Configuration** menu and clicking on the **static NAT** button.



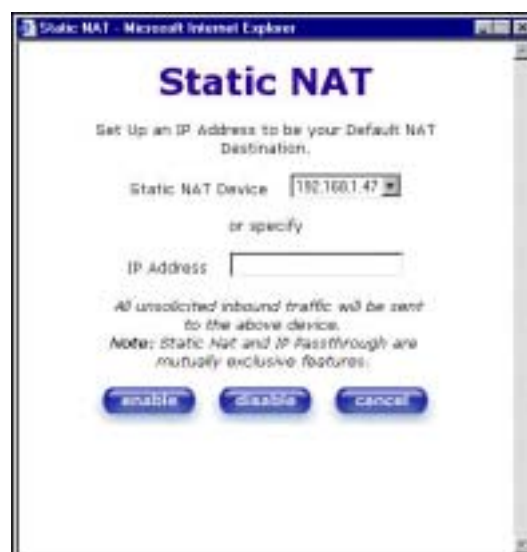
## 13.6 Enabling Static NAT

Before you enable static NAT, you must select **Default** from the **Current Profile** drop-down box. Static NAT must be configured for the Gateway's default account profile. After you select the default profile, click the **static NAT** button.

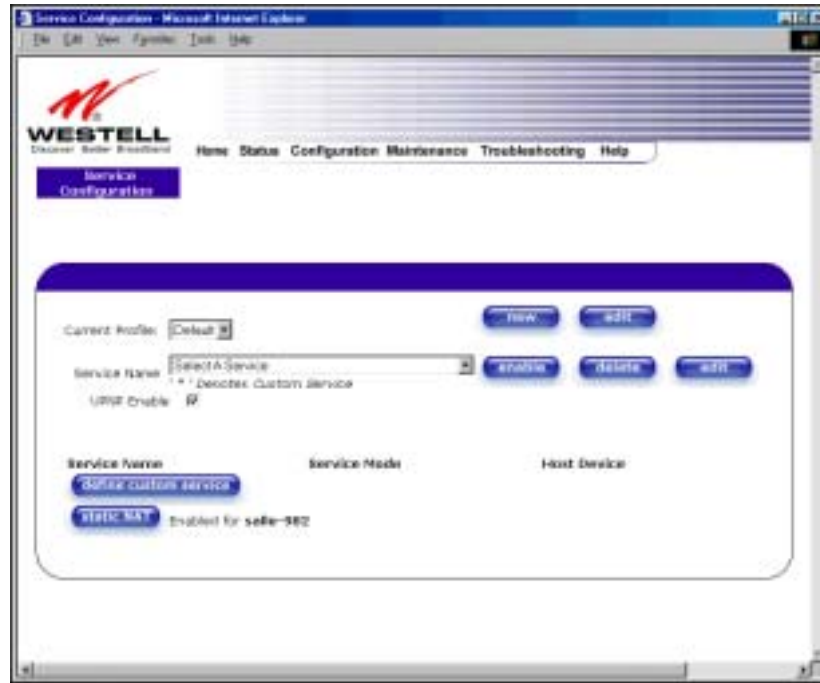
**NOTE:** In the following screen, the default account profile is labeled **Default**. However, if you have renamed the default account profile, you must select the profile name you created as the default profile.



If you click on the **static NAT** button in the **Service Configuration** screen, the following screen will be displayed. Select your device from the **Static NAT Device** drop-down arrow, or type the IP address of the device in the field labeled **IP Address**. Click on **enable**. This will automatically enable the Static NAT feature for that device.



If you click **enable**, the following Service Configuration screen will display. Static NAT is now enabled for the device you selected.

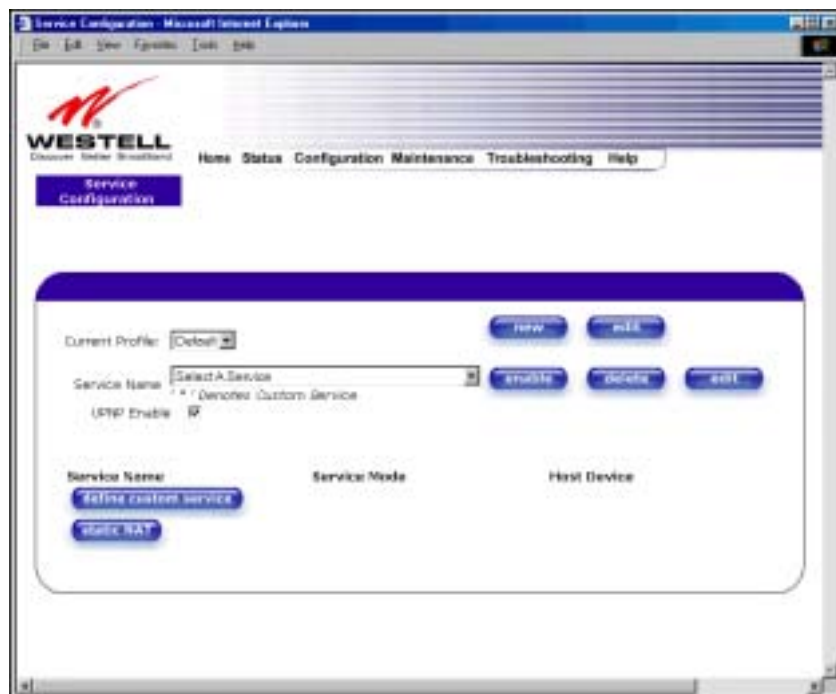


## 13.7 Disabling Static NAT

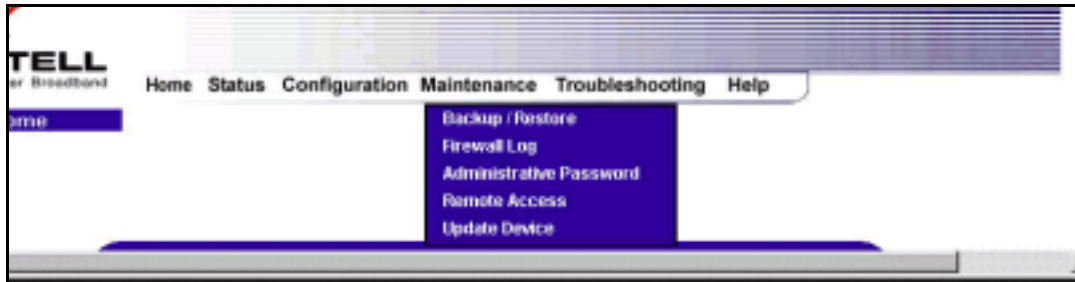
If you click on **static NAT** in the **Service Configuration** screen, the following screen will be displayed, select a device name from the **Static NAT Device** drop-down arrow, or type the IP address of the device in the field labeled **IP Address**. Click on **disable**. This will automatically disable the Static NAT feature for that device.



If you click **disable**, the following Service Configuration screen will be displayed. Static NAT is now disabled for the device you selected. (No device is displayed in the field adjacent to the **static Nat** button.)



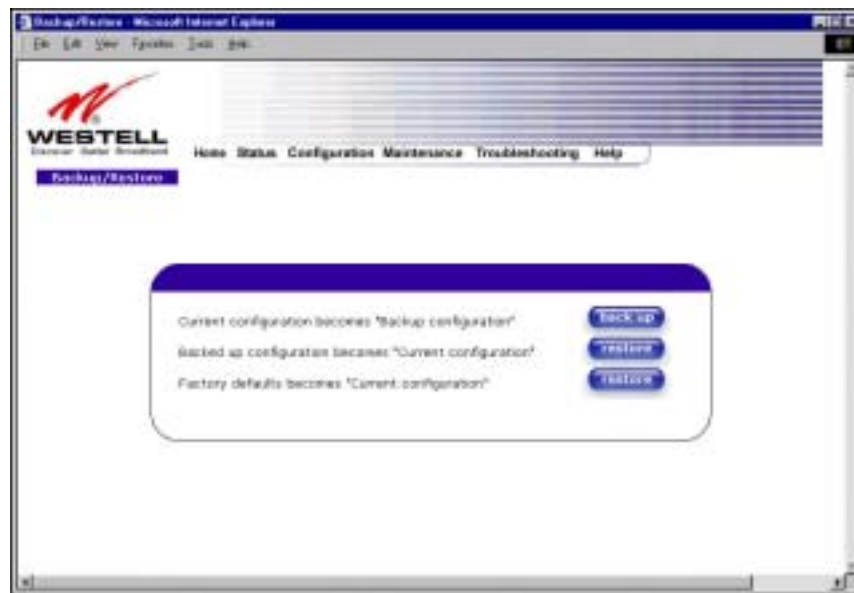
## 14. MAINTENANCE



### 14.1 Backup/Restore

The following settings will be displayed if you select **Backup/Restore** from the **Maintenance** menu.

NOTE: Backup settings are stored in a separate area of flash, not to an external backup source.



Current configuration becomes Backup Configuration	Select this button if you want to store all of the current configuration data such that it can be recalled later.
Backed up configuration becomes Current configuration	Select this button if you want to retrieve the last back up copy of all configuration parameters and make these values current.
Factory default becomes Current configuration	Select this button if you want set all user configurable parameters back to the factory default.

## 14.2 Firewall Log

The following settings will be displayed if you select **Firewall Log** from the **Maintenance** menu.

This screen is an advanced diagnostics screen. It alerts you of noteworthy information sent to VersaLink from the Internet. The screen can contain 1000 entries, but a maximum of 50 entries are displayed at a time. Once 1000 entries have been logged, the oldest entry is removed to make space for the new entries as they occur. The following settings are displayed.



Clear log	Selecting this button removes all entries from the log.
Printable/savable format	Selecting this button opens a new window that contains a list of all the logged packets that can be saved or printed.
Settings	Selecting this button opens a new window that contains configuration settings for selecting the information that you want logged.
Packet	The packet number.
Date	The number of days passed since that the packet was sent.
Time	The time that the packet was sent.
Direction/Source	The direction of transmission.
Rule/Reason	The internal rule that caused the logged event. The internal rule is set up under Firewall rules.
Alert	Displays a description of the logged event.

If you clicked on **details** in the **Firewall Log** screen, the **Packet Details** screen will be displayed. Click on **close**.



To clear the Firewall log, click **clear log** in the **Firewall Log** screen. The following pop-up screen will be displayed. Click **OK** when asked "Do you wish to clear the Firewall log file?" If you click **Cancel**, the firewall log will not be cleared.



To obtain a printable format of the Firewall Log, at the **Firewall Log** screen, click **Printable/Savable Format**. This will allow you to send a copy of the Firewall log to your designated printer.

## 14.3 Administrative Password

The following settings will be displayed if you select **Administrative Password** from the **Maintenance** menu. After you enter your data into the appropriate settings, click on **change**.

NOTE: If the Gateway is password protected and you are not an authorized user, you will not be able to change the values. (The Gateway cannot be configured unless the user is logged in.) Contact your network administrator for further instructions.

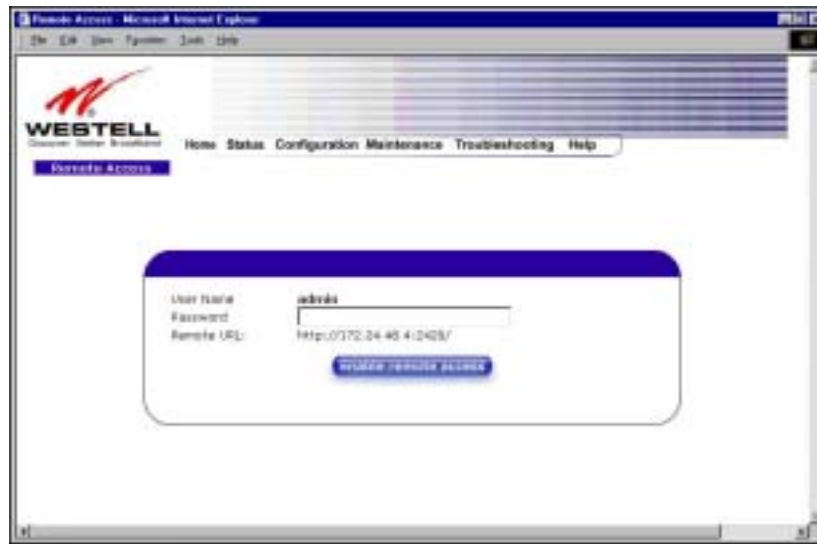


Enter Administrative Name NOTE: This changes the Systems Administrator password not the PPP password.	Type the name of your network administrative.
Enter Administrative Password	Type your network administrator's password.
Verify Administrative Password	Re-type your network administrator's password.

## 14.4 Remote Access

The following screen will appear if you select **Remote Access** from the **Maintenance** menu. To enable Remote Access, type in a password and click the **enable remote access** button.

**NOTE:** The password should be at least 4 characters long and should not exceed 32 characters. Do not type a blank space or asterisks in the Password field. The password is also case sensitive.



User Name	Displays your current User Name (Static field)
Password	Field for entering your password
URL	Displays the IP address of the remote management VersaLink

The following screen displays a message that the remote access is currently enabled. After 20 minutes of inactivity, or on reboot, remote access will be automatically disabled. To disable remote access, click on the **disable remote access** button.



## 14.5 Update Device

The following screen will be displayed if you click on **Update Device** from the **Maintenance** menu. This screen is used to update the firmware that controls the operation of VersaLink. The updated firmware may be loaded from either a file that is located on your PC's hard drive or from update files stored on an Internet server.

**NOTE:** The configurable settings of your Gateway may be erased during the update process.

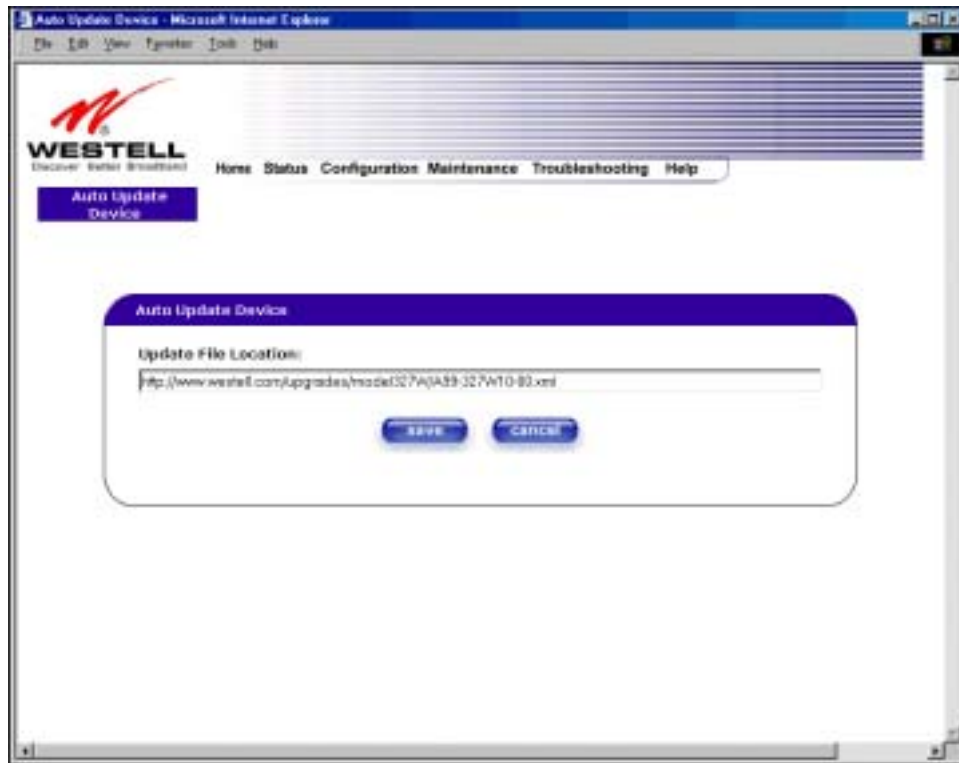


Click on the **check for web update** button in the **Update Device** screen to check the web for possible software updates. This screen will retrieve the software update file and display any available update information. You must be connected to the Internet to use this option.

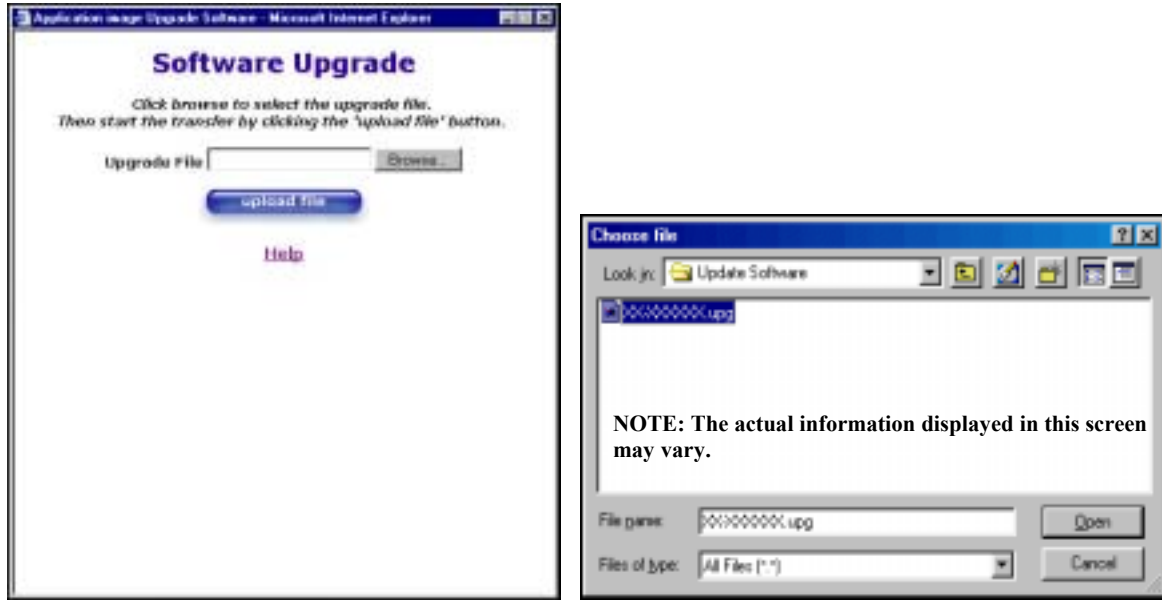
NOTE: If you click on check for web update and the page returns a “page not found” message, this indicates that the software update file is not available. Go back to the previous screen to continue.

Click on the **web update now** button in the **Update Device** screen to download the software update file and automatically update the modem firmware if an update is available and applicable. You must be connected to the Internet to use this option.

If you click on the **settings** button in the **Update Device** screen, the following screen will appear. This screen displays the location of the software update file.



Click on the **local update now** button in the **Update Device** screen to select the upgrade file from your PC's hard drive. This screen allows you to upgrade the software on VersaLink. Click **Browse...** and go to the location where the upgrade file is stored.



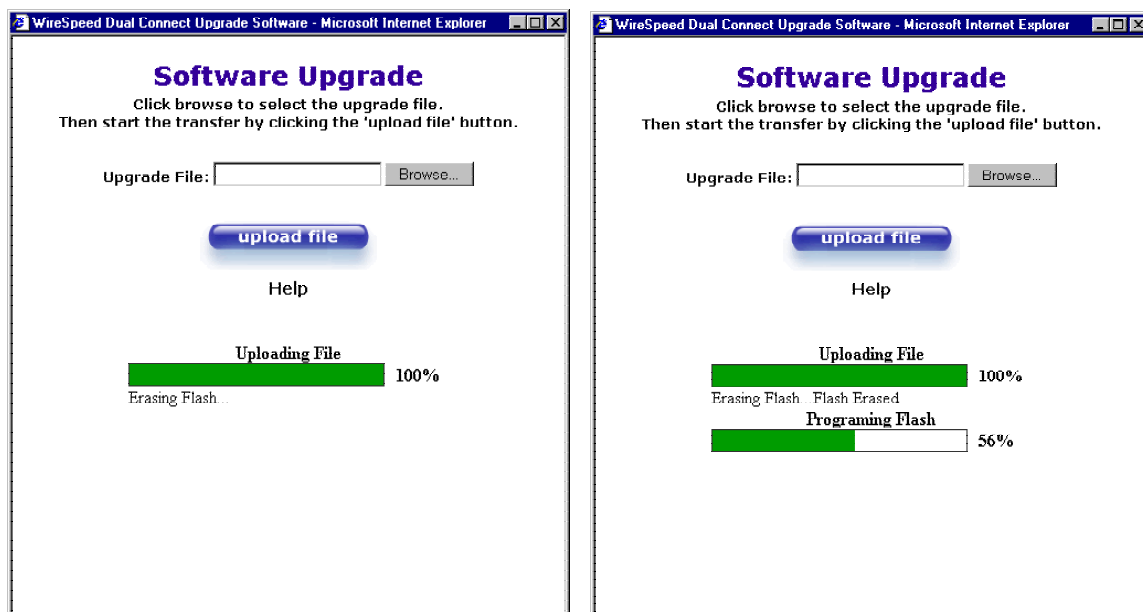
Select the appropriate upgrade file from your browser. The file name will appear in the field labeled **Upgrade File**. Click on **upload file**.



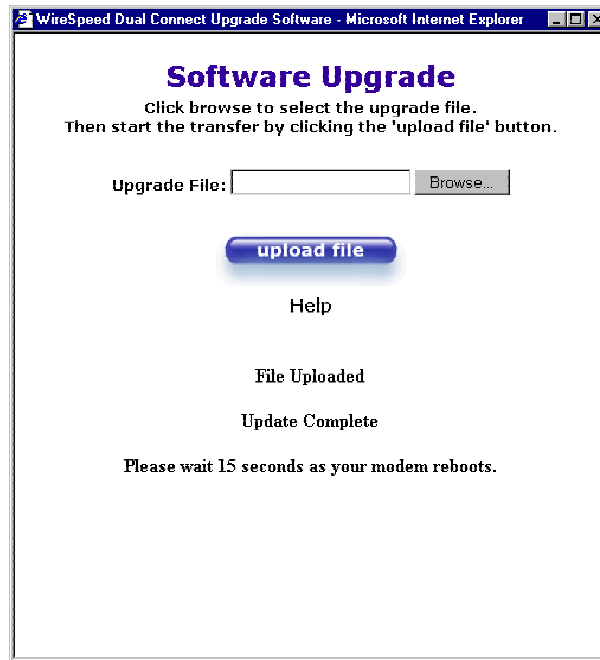
This screen shows that the file is being uploaded to VersaLink.



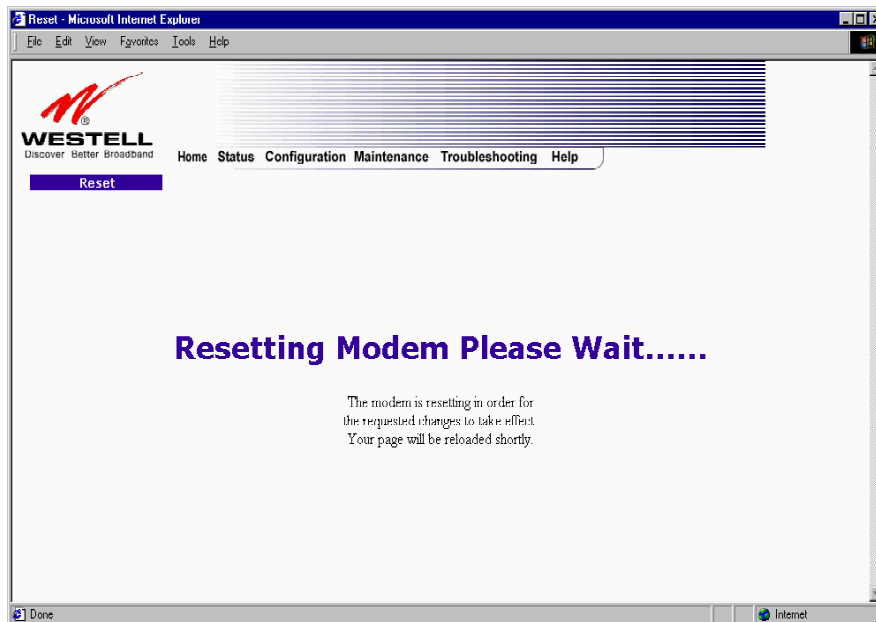
The screens below show that the file upload has completed and that the Programming Flash is being erased to prepare the Flash storage area for upload of the new file. (Programming Flash is a temporary storage area for uploaded files.)



The screen below shows that the upload was successful. The Gateway will not reboot.



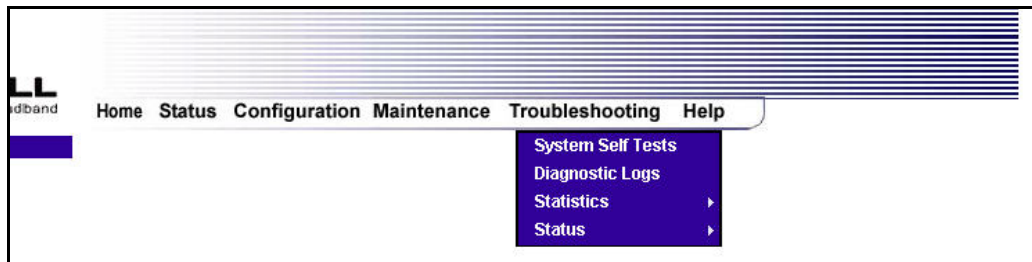
The following screen will be displayed as VersaLink is being reset.



After a brief delay, the home page will be displayed. Confirm that you have a DSL sync and that the PPP Status displays **UP**. (Click on the **reset** button to re-establish your PPP session.)

## 15. TROUBLESHOOTING

NOTE: Options in the **Troubleshooting** menu may or may not be displayed depending on VersaLinks WAN Configuration (DSL/ATM PORT or ETHERNET PORT 1). However, all menu options are displayed if VersaLink is configured for DSL/ATM PORT 1. The following sections provide further details on the Troubleshooting menu.



### 15.1 System Self Tests

The following settings will be displayed if you select **System Self Tests** from the **Troubleshooting** menu. Click on **test all** to run a diagnostic test on VersaLink's connection.



If you want to PING using the System Self Test screen (diagnostics page) shown above, enter your **DNS** or **IP** address in the fields provided and click on the **test** button. The System Self Test will run a diagnostic test that executes independent of firewall security settings. See the following table for test descriptions and possible responses.

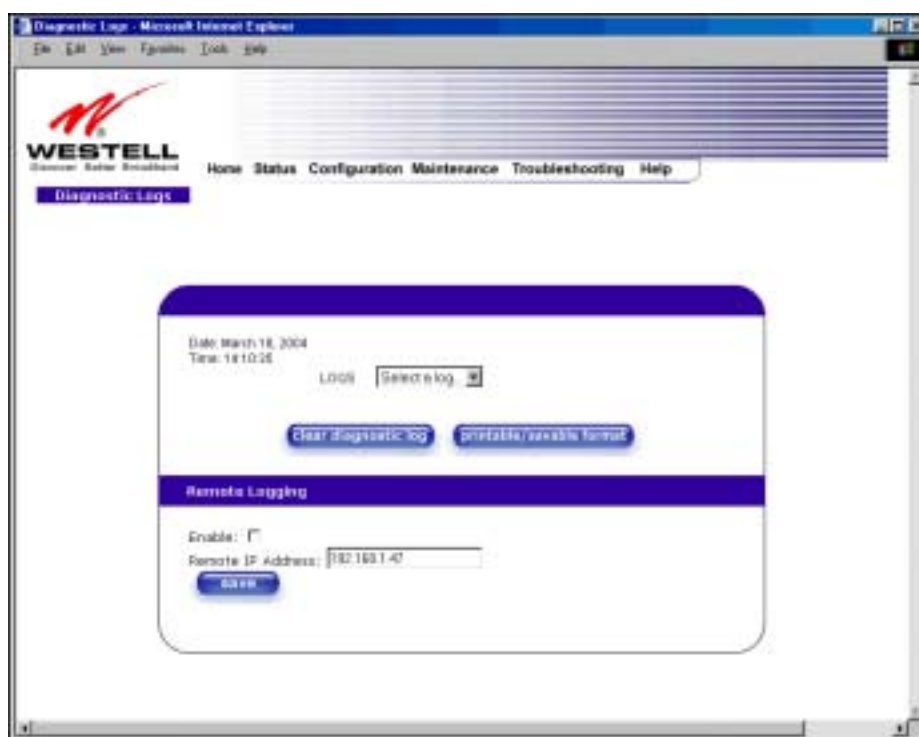
If you want to PING using the MS-DOS (shell) window, first you will need to check your firewall security setting. (If you PING via DOS shell you are susceptible to firewall rules, as this PING is dependent on VersaLink's firewall settings.) If your firewall is set to **Medium** or **High**, you will not be able to PING. You must set your firewall security setting to **Low** or **None**.

Connection/Status	
DSL	<p>VersaLink checks the status of the DSL connection.</p> <p>Possible responses are:  UP: VersaLink is operating correctly and has obtained synchronization with the opposing network device.  DOWN: VersaLink is operating correctly, but has not synchronized with the opposing device.</p>
PPPoE	<p>Indicates that a PPPoE session is or is not established.</p> <p>Possible responses are:  Session UP: A valid PPPoE session has been detected.  No Session: Currently there is no active PPPoE session established.  Initiating Session: A PPP session must be connected from the homepage screen.</p>
PPP	<p>Indicates that a PPPoE or PPPoA session must already be established.</p> <p>Possible responses are:  Connection UP: VersaLink has established a connection  No Connection: There is no PPP connection  Initiating Connection: The PPP connection process has been initiated  Connection Halted: A successful PPP connection was halted  Cannot Connect: A PPP connection could not be made because of a PPPoE session failure.  Authorization Failure: The user name or password is incorrect.  Link Control Protocol Failed: Re-establish the session (from the home page).</p>
Test Description / Test Results	
Self Test	Performs an integrity check of certain internal components of VersaLink.
PING ISP's VersaLink	<p>Performs an IP network check (i.e., an IP Ping) of the Service Provider's VersaLink. This test verifies that VersaLink can exchange IP traffic with an entity on the other side of the DSL line.</p> <p>Possible responses are:  Success: VersaLink has detected an IP Remote VersaLink connection.  No Response: The IP Remote VersaLink does not answer the IP Ping.  Could not test: The test could not be executed due to VersaLink settings. Check your DSL sync or your PPP session. You must have both a DSL sync and a PPP connection established to execute a PING.</p>
DNS	<p>Performs a test to try to resolve the name of a particular host. The host name is entered in the input box.</p> <p>Possible responses are:  Success: VersaLink has successfully obtained the resolved address. The IP address is shown below the host name input box.</p>

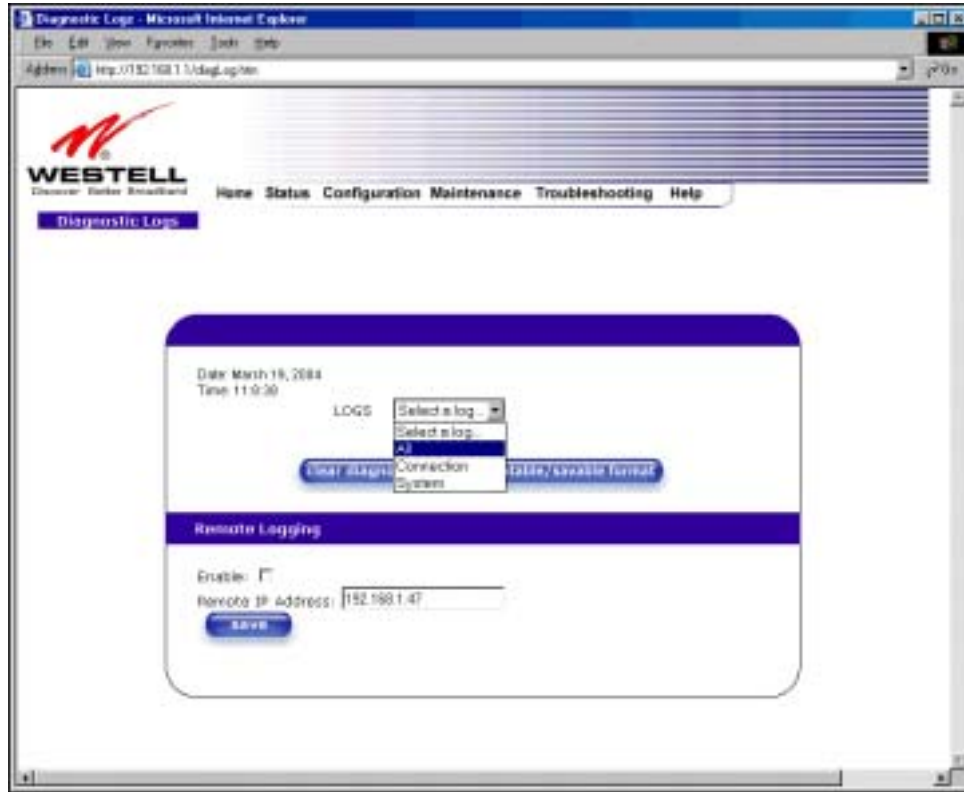
	<p>No Response: VersaLink has failed to obtain the resolved address.</p> <p>Host not found: The DNS Server was unable to find an address for the given host name.</p> <p>No data, enter host name: No host name is specified.</p> <p>Could not test: The test could not be executed due to VersaLink settings. Check your DSL sync or your PPP session. You must have both a DSL sync and a PPP connection established to execute a PING.</p>
IP Address	IP Address of the Host Name.
PING (via IP Address or Host Name)	<p>Performs an IP connectivity check to a remote computer either within or beyond the Service Provider's network. You can PING a remote computer via the IP address or the DNS address. If your PING fails, try a different IP or DNS address.</p> <p>Possible responses are:</p> <p>Success: The Remote Host computer was detected.</p> <p>No Response: There was no response to the Ping from the remote computer.</p> <p>No name or address to PING: No host name or IP address was specified.</p> <p>Could not test: The test could not be executed due to VersaLink settings. Check your DSL sync or your PPP session. You must have both a DSL sync and a PPP connection established to execute a PING.</p>
Trace	<p>Determines the route taken to destination by sending Internet Control Message Protocol (ICMP) echo packets with varying IP Time-To-Live (TTL) values to the destination. Trace Route is used to determine where the packet is stopped on the network.</p>

## 15.2 Diagnostic Logs

If you select **Diagnostic Log**, from the **System Self Test** menu, the following screen will be displayed.



To see a list of the log options, click on the arrow at the **LOGS** drop-down menu. Select an option from the list provided at the **Diagnostics Logs** screen.

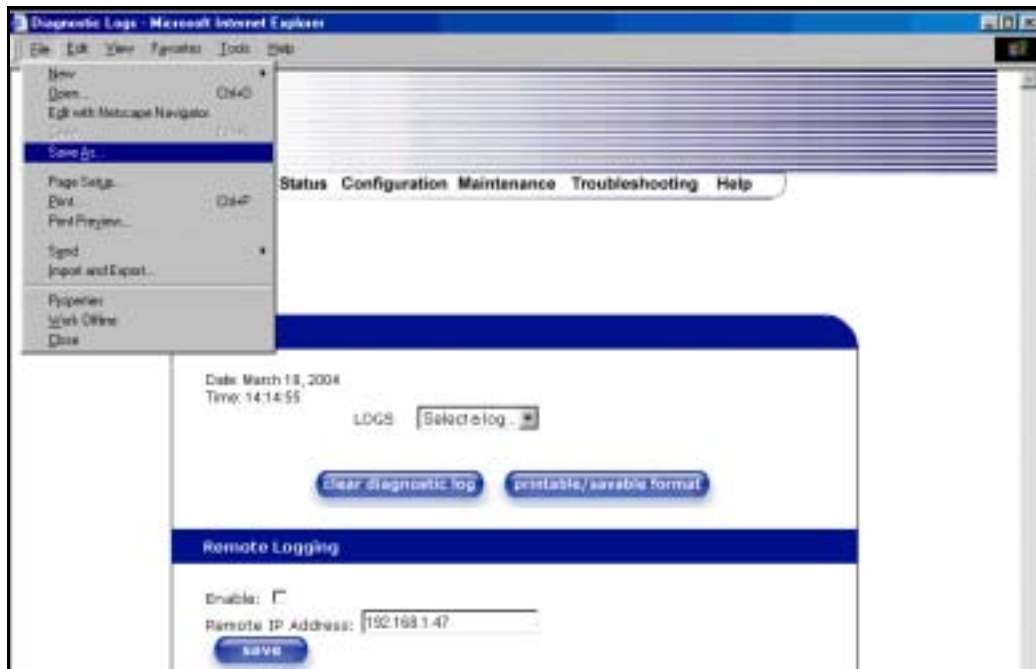


If you clicked on **All**, the following screen will be displayed. This screen provides a detailed list of VersaLink's connection status and system information. Click on **clear diagnostic log** to clear the diagnostic log information.

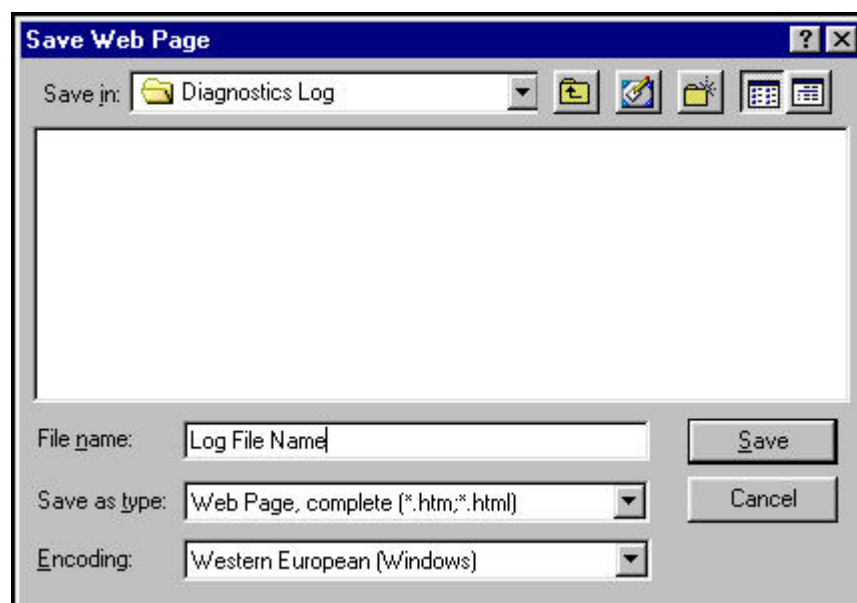


## 15.2.1 Saving the Diagnostic Log File

If you want to save the diagnostic log file, go to your Browser's menu and select **File**, then select **Save As** from the drop-down menu.

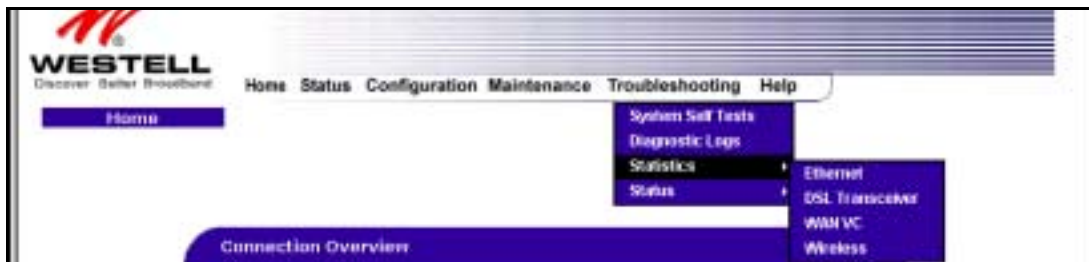


At the **Save Web Page** dialog box, select a destination for your log file from the **Save in** drop-down arrow. Next, enter a name for your log file in the field labeled **File name** and click on **Save**.



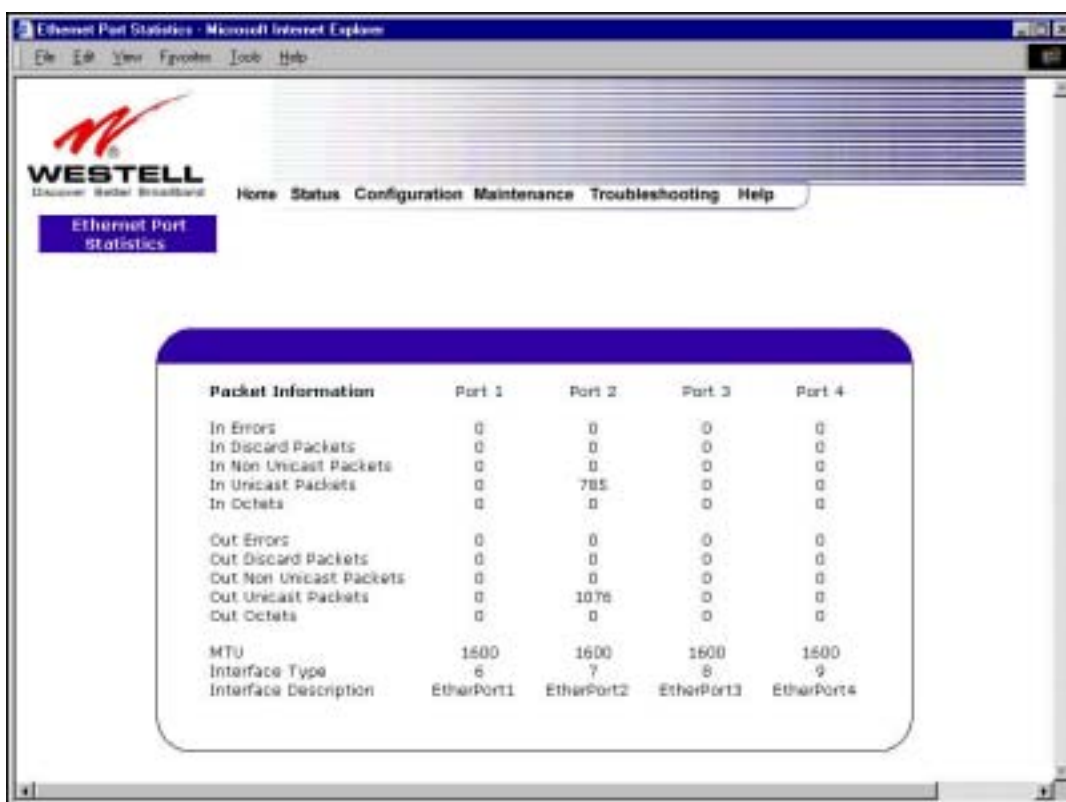
## 15.3 Statistics

NOTE: If VersaLink is configured for **ETHERNET PORT 1**, only **Ethernet** and **Wireless** statistics will be displayed in the **Statistics** menu. The **DSL Transceiver** statistics and the **WAN VC** statistics will not be displayed. If you want to view **DSL Transceiver** and **WAN VC** statistics, you must configure VersaLink for **DSLATM PORT**. Refer to section 12.6.2.1 for additional details.



### 15.3.1 Ethernet Port Statistics

The following settings will be displayed if you select **Ethernet** from the **Statistics** menu.



The screenshot shows the 'Ethernet Port Statistics' page in a Microsoft Internet Explorer browser window. The page displays a table of statistics for four Ethernet ports (Port 1, Port 2, Port 3, and Port 4). The table includes columns for Packet Information and the corresponding statistics for each port. The statistics are as follows:

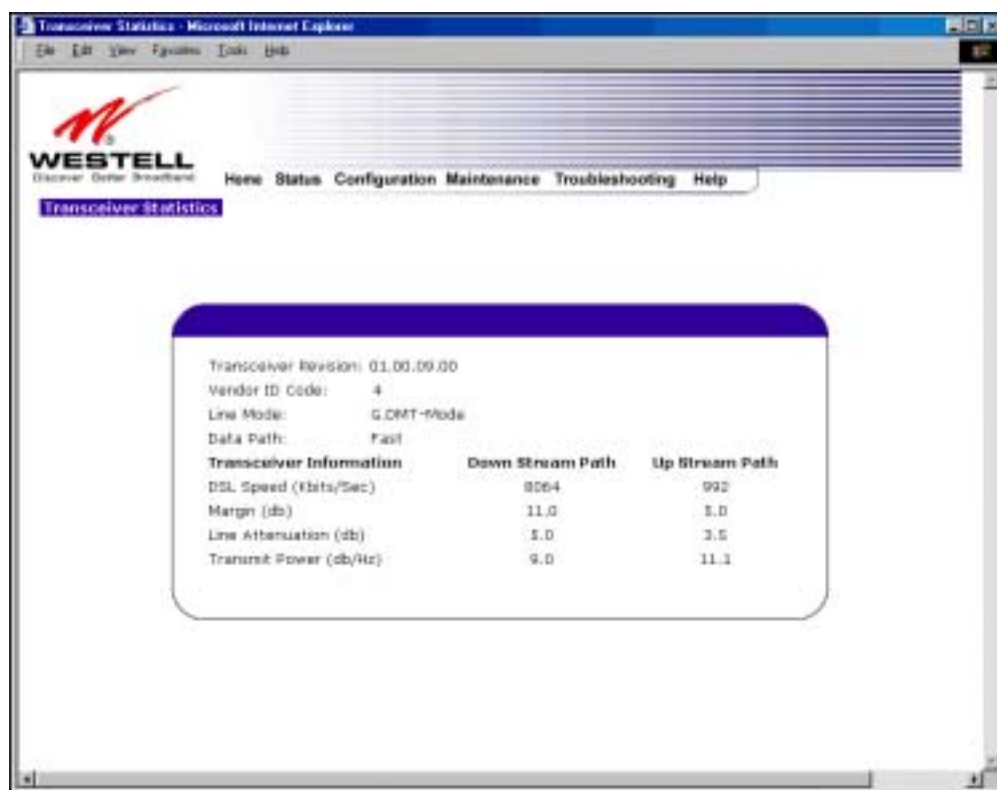
Packet Information	Port 1	Port 2	Port 3	Port 4
In Errors	0	0	0	0
In Discard Packets	0	0	0	0
In Non Unicast Packets	0	0	0	0
In Unicast Packets	0	785	0	0
In Octets	0	0	0	0
Out Errors	0	0	0	0
Out Discard Packets	0	0	0	0
Out Non Unicast Packets	0	0	0	0
Out Unicast Packets	0	1076	0	0
Out Octets	0	0	0	0
MTU	1500	1600	1600	1500
Interface Type	6	7	8	9
Interface Description	EtherPort1	EtherPort2	EtherPort3	EtherPort4

In Errors	The number of error packets received on the Ethernet interface.
In Discard Packets	The number of discarded packets received.
In Non Unicast Packets	The number of non-Unicast packets received on the Ethernet interface.
In Unicast Packets	The number of Unicast packets received on the Ethernet interface.
In Octets	The number of bytes received on the Ethernet interface.
Out Errors	The number of outbound packets that could not be transmitted due to errors.
Out Discard Packets	The number of outbound packets discarded.
Out Non Unicast Packets	The number of non-Unicast packets transmitted on the Ethernet interface.
Out Unicast Packets	The number of Unicast packets transmitted on the Ethernet interface.
Out Octets	The number of bytes transmitted on the Ethernet interface.
MTU	Maximum Transmission Unit- The number of data bytes contained in the Ethernet frame.
Interface Type	A unique identifier that represents the interface type.
Interface Description	A description field that refers to the interface type.

## 15.3.2 DSL Transceiver Statistics

The following settings will be displayed if you select **DSL Transceiver** from the **Statistics** menu.

NOTE: If VersaLink is configured using **ETHERNET PORT 1**, the following screen will not be available.



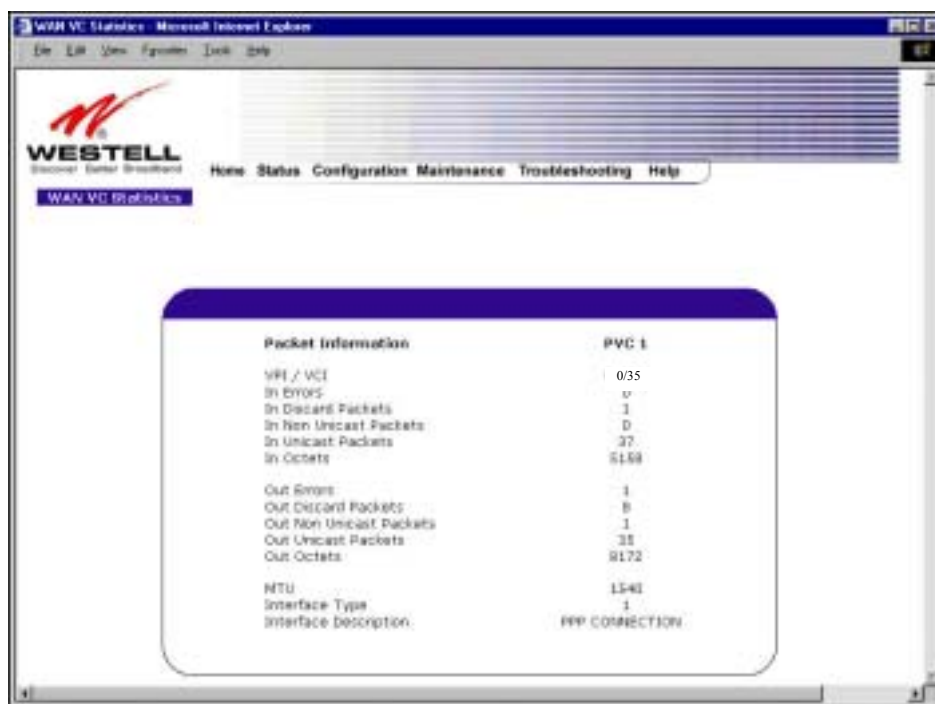
Transceiver Revision	The transceiver software version number.
Vendor ID Code	The CPE Vendor's ID code for their chipset.
Line Mode	The operational mode. Modes supported are No Mode, Multi Mode, T.1413 Mode, G.DMT Mode, and G.LITE Mode.
Data Path	The data path used (either Fast or Interleaved).

Transceiver Information-Down Stream/Up Stream Path	
DSL Speed (Kbits/Sec)	The transmission rate that is provided by your Internet Service Provider (ISP).
SNR Margin (db)	The Signal-to-Noise Ratio (S/N) where 0 db = $1 \times 10^{-7}$ , which inhibits your DSL speed.
Line Attenuation (dB)	The DSL line loss.
Transmit Power (db/Hz)	The transmitted signal strength.

### 15.3.3 WAN VC Statistics

The following settings will be displayed if you select **WAN VC** from the **Statistics** menu.

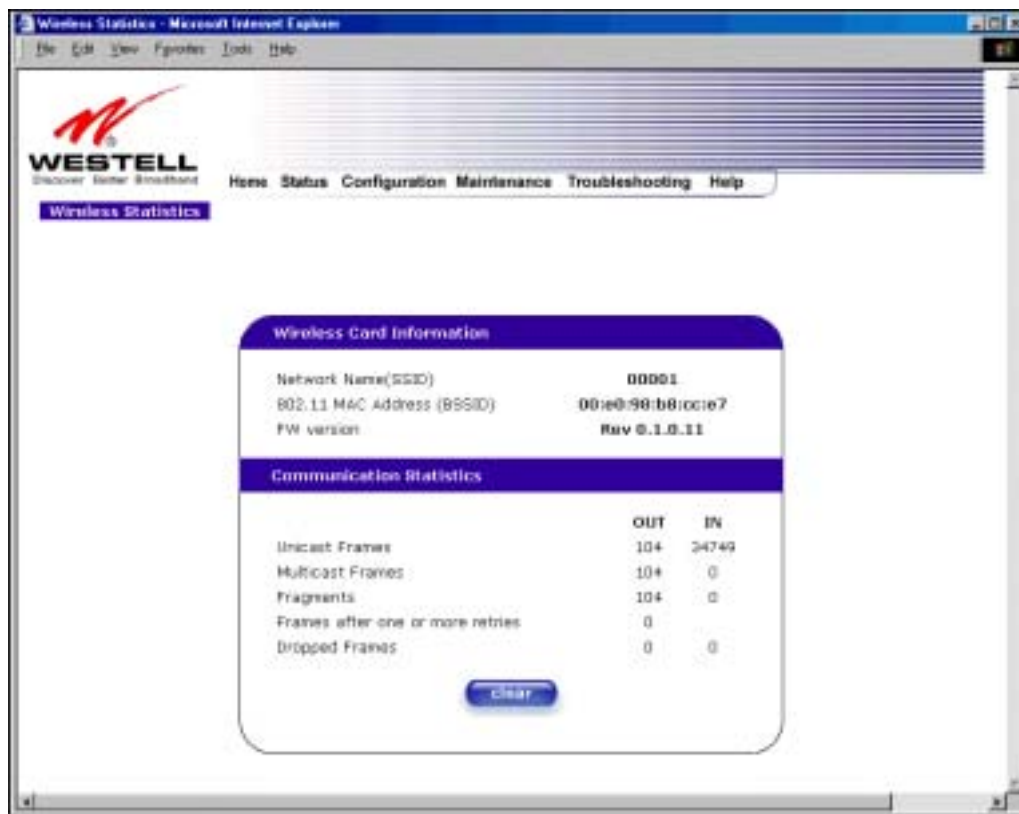
NOTE: If VersaLink is configured using **ETHERNET PORT 1**, the following screen will not be available.



VPI/VCI	Displays the VPI/VCI values obtained from your Internet Service Provider.
In Errors	The number of error packets received on the ATM port.
In Discard Packets	The number of discarded packets received.
In Non Unicast Packets	The number of non-Unicast packets received on the ATM port.
In Unicast Packets	The number of Unicast packets received on the ATM port.
In Octets	The number of bytes received on the ATM port.
Out Errors	The number of outbound packets that could not be transmitted due to errors.
Out Discard Packets	The number of outbound packets discarded.
Out Non Unicast Packets	The number of non-Unicast packets transmitted on the ATM port.
Out Unicast Packets	The number of Unicast packets transmitted on the ATM port.
Out Octets	The number of bytes transmitted on the ATM port.
MTU	Maximum Transmission Unit -The number of data bytes contained in the ATM frame.
Interface Type	A unique identifier that represents the interface type.
Interface Description	A description field that refers to the interface type.

## 15.4 Wireless Statistics

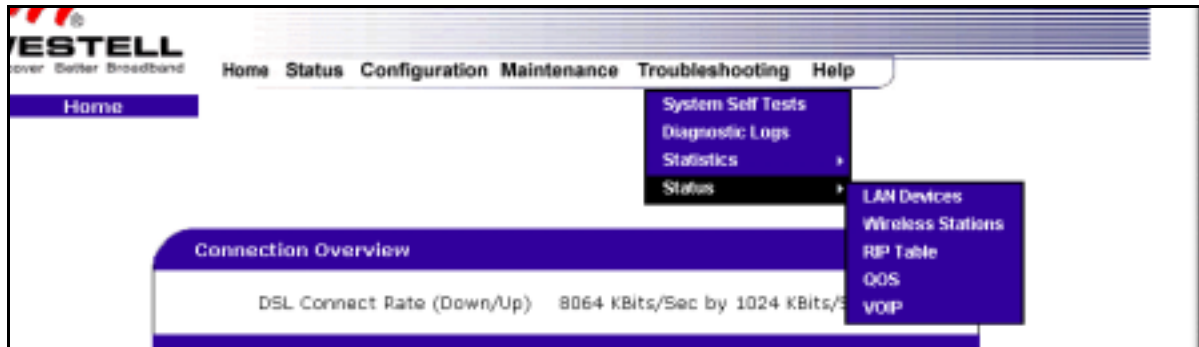
The following settings will be displayed if you select **Wireless** from the **Statistics** menu.



Wireless Card Information	
<b>Network Name (SSID)</b>	This string, (32 characters or less) is the name associated with the Access Point (AP). To connect to the AP, the Service Set ID (SSID) on a Station card must match the SSID on the AP.
<b>802.11 MAC Address (BSSID)</b>	This is the Media Access Controller address of the AP. It is used as the Basic Service Set Identifier (BSSID).
<b>FW Version</b>	This is the Network Interface Card Identifier. It uniquely identifies the hardware platform of the AP. This is used with other information to determine if the inserted card can be used as an AP, and if so, the version of AP firmware to be used. Not all makes of wireless station cards can be used as an AP.
Communication Statistics	
NOTE: Data preceded by <b>OUT</b> pertain to transmissions from the VersaLink to a station; VersaLink is the source. Data preceded by <b>IN</b> pertain to data received by VersaLink; VersaLink is the destination.	
<b>OUT-Unicast Frames</b>	The number of successfully transmitted frames whose destination address was a single station; not necessarily the same station, but to any single station as opposed to a transmission that multiple stations would receive-as in the case of broadcast message.
<b>OUT-Multicast Frames</b>	The number of successfully transmitted frames whose destination address was a multicast address (received by more that one station): not necessarily

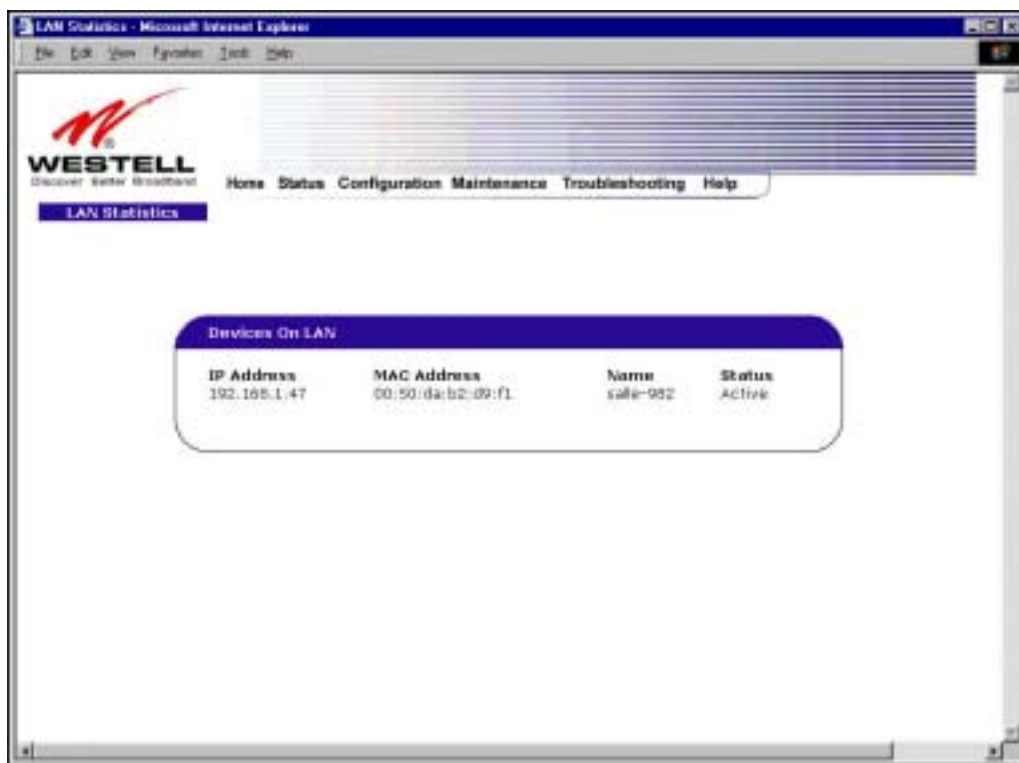
	broadcast to all stations, but more than a single station. Broadcast messages are included in the count.
<b>OUT-Fragments</b>	The number of successful transmissions made. This will typically be greater than the sum of the Unicast and Multicast frames because large frames are broken into multiple transmissions. The number of fragments per frame is based on the Fragmentation Threshold setting (not user-configurable).
<b>OUT-Frames after one or more retries</b>	The number of frames that successfully transmitted after more than one retry. Any fragment of a frame that required multiple retries would increment this counter for the whole frame.
<b>OUT-Dropped Frames, too many retries</b>	The number of frames that did not transmit due to the short or long retry limit being reached because no acknowledgement or CTS was received.
<b>IN-Unicast Frames</b>	The number of successfully received frames whose destination address was a single location, not necessarily the same location, but to any single location as opposed to the broadcast address.
<b>IN-Multicast Frames</b>	The number of successfully received frames whose destination address was a multicast address. Broadcast messages are included in this count.
<b>IN-Fragments</b>	The number of fragments successfully received. This may not be equal to the sum of the Unicast and Multicast frames because large frames are broken into multiple transmissions. The number of fragments per frame is based on the Fragmentation Threshold setting (not user-configurable) on the source station.
<b>IN-Frames after one or more retriee</b>	The number of frames that successfully transmitted after more than one retry. Any fragment of a frame that required multiple retries would increment this counter for the whole frame.
<b>IN-Drops due to insufficient Rx buffers</b>	The number of received frames discarded due to lack of buffer space.

## 15.5 Status



### 15.5.1 LAN Devices

The following settings will be displayed if you select **LAN Devices** from the **Status** menu.



Devices on LAN	
IP Address	Displays the IP network address that VersaLink is on.
MAC Address	Media Access Controller (MAC) address of this device.
Name	Displays the ASCII (text) name of the devices connected to the LAN.
Status	Displays the status of the devices connected to the LAN.

## 15.5.2 Wireless Stations

The following settings will be displayed if you select **Wireless** from the **Status** menu.

NOTE: A Wireless device must be connected to the Gateway for the fields in this screen to be populated.

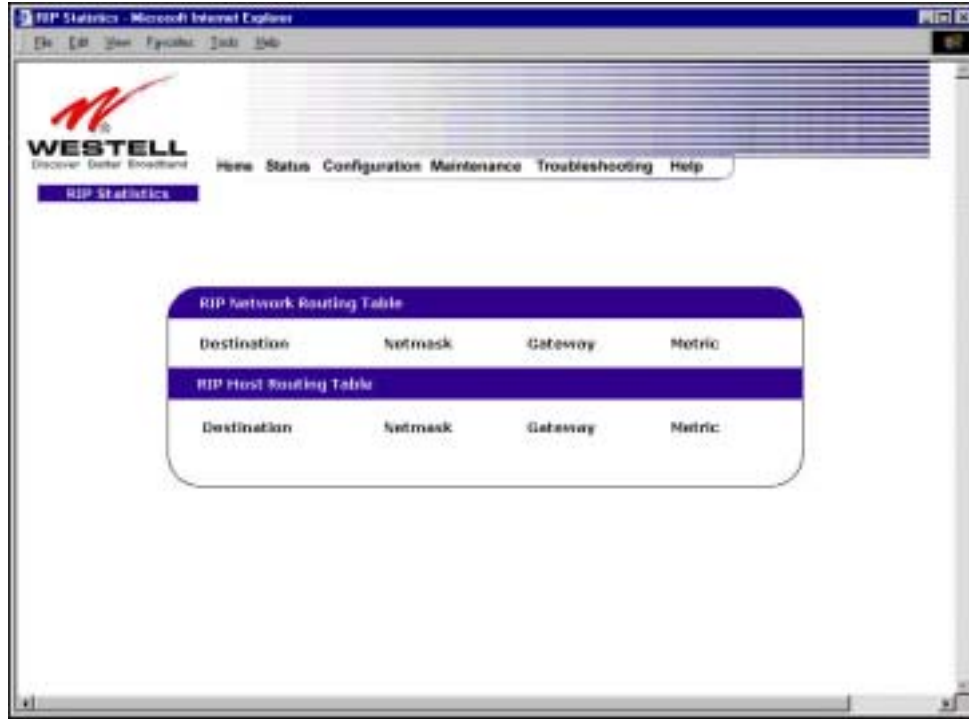


Wireless Stations List	
Station	This number indicates the order in which the stations are first accessed by VersaLink.
MAC Address	The Media Access Controller Address assigned to the station.
State	The current state of the negotiation between the station and VersaLink.
PBCC	Indicates whether the station that is associated with VersaLink operates in PBCC (Packet Binary Convolutional Code) modulation.
Active Rate	The current transmit and receive rate.

### 15.5.3 RIP Table

The following settings will be displayed if you select **RIP Table** from the **Status** menu.

NOTE: RIP must be enabled for this table to be populated.

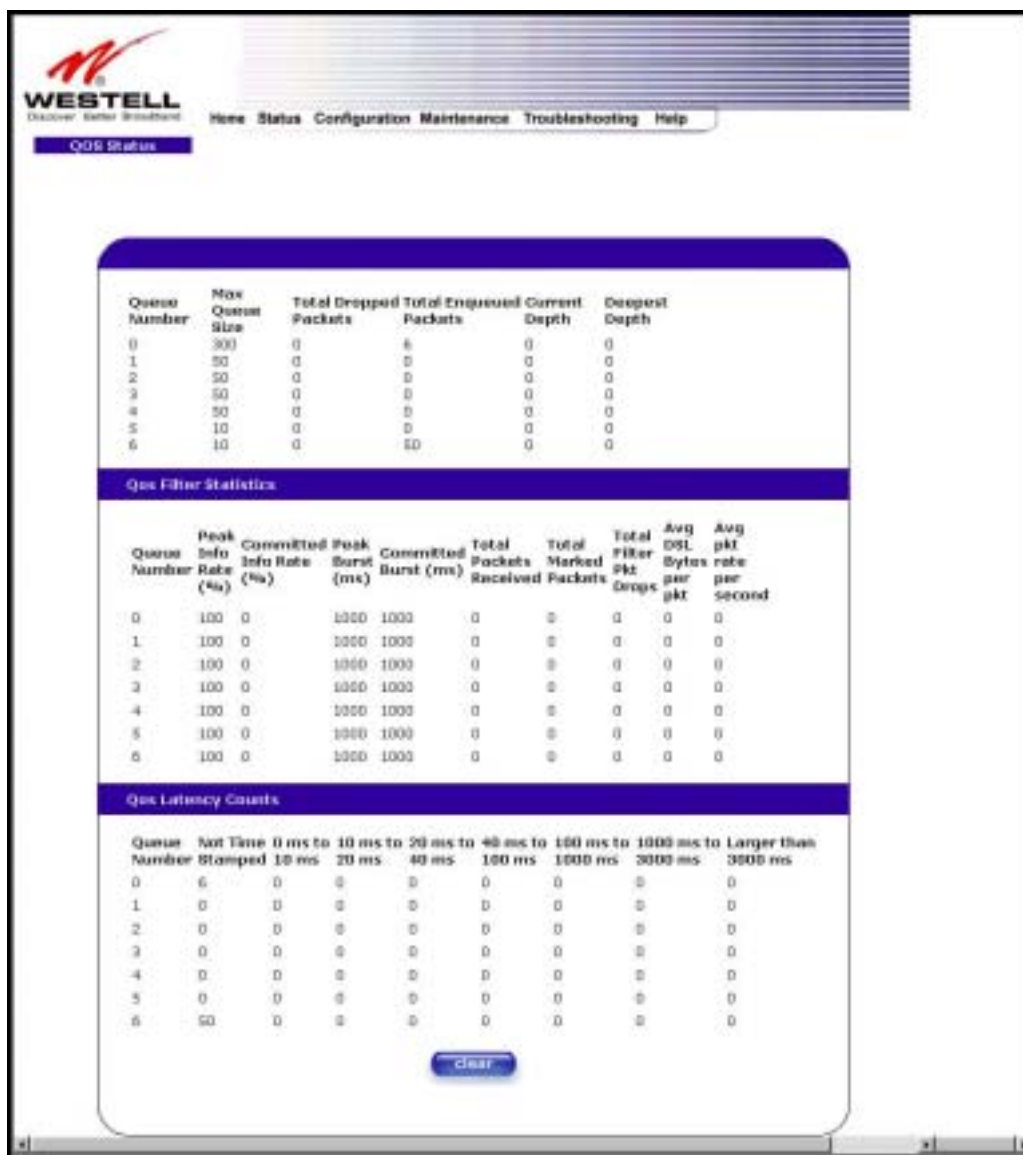


RIP Network Routing Table	Indicates Network routes received via RIP.
RIP Host Routing Table	The Host routes received via RIP.
Destination	The destination IP address of the route
Netmask	The IP mask of the route
Gateway	The gateway of the route
Metric	The RIP metric (0-15). A lower value is better.

## 15.5.4 QOS Status

The following settings will be displayed if you select **QOS** from the **Status** menu. Click on the **clear** button to clear all counts and statistics (not just latency counts). This does not affect the configuration values.

NOTE: QoS must be enabled on the Gateway for this table to be populated.



Queue Number

Indicates the DiffServ Queue.  
Possible responses are:  
0 = Best Effort (BE)  
1 = Assured Forwarding 1 (AF1)  
2 = Assured Forwarding 2 (AF2)  
3 = Assured Forwarding 2 (AF3)  
4 = Assured Forwarding 2 (AF4)

	5 = Expedited Forwarding (EF) 6 = Routing Protocols (DiffServ priorities 6 and 7)
Max Queue Size	The maximum number of packets that can be queued for this priority.
Total Dropped Packets	Indicates how many packets of this priority have been dropped by QOS due to lack of buffer space or filtering rules.
Total Enqueued Packets	Displays the number of packets, destined for the WAN, that have been received.
Current Depth	Displays the current number of packets of this priority that are queued.
Deepest Depth	Displays the most number of packets that have been queued at once for this priority.
<b>QOS Filter Statistics</b>	
Queue Number	The DiffServ Queue. (See Queue Number description above.)
Peak Info. Rate (%)	The maximum allowed rate for this priority, expressed as a percentage of the DSL rate.
Committed Info Rate (%)	The committed rate for this priority, expressed as a percentage of the DSL rate
Peak Burst (ms)	Displays the interval in milliseconds for averaging the peak offered rate.
Committed Burst (ms)	Displays the interval in milliseconds for averaging the committed offered rate.
Total Packets Received	Displays the total number of packets of this priority that are destined for the LAN.
Total Marked Packets	Displays the number of packets of this priority that exceeded the committed rate, but not the peak rate, and were marked with a higher drop priority
Total Filter Packet Drops	Displays the number of packets of this priority that exceeded the peak rate and that were, therefore, dropped.
Avg. DSL Bytes Per Packet	Displays the average size of packets for this priority, including all overhead.
Avg. Packet Rate Per second	Displays the average rate (in packets per seconds) for this priority.
<b>QOS Latency Counts</b>	
Queue Number	The DiffServ Queue. (See Queue Number description above.)
Not Time Stamped	The packets with no incoming time stamp. (Often these are generated internal to the modem.)
A ms to B ms	<p>The number of packets of this priority whose time in the modem fell between A and B milliseconds. (Time is measured from the point the packet arrives at the modem's processor until is passed to the ATM hardware for transmission.)</p> <p>Possible ranges are (A ms to B ms):</p> <ul style="list-style-type: none"> <li>0 ms to 10 ms</li> <li>10 ms to 20 ms</li> <li>20 ms to 40 ms</li> <li>40 ms to 100 ms</li> <li>100 ms to 1000 ms</li> <li>1000 ms to 3000 ms</li> <li>Larger than 3000 ms</li> </ul>

## 15.5.5 VOIP Status

The following settings will be displayed if you select **VOIP** from the **Status** menu.

NOTE: A VOIP device must be connected to the Gateway for this table to be populated.



SIP Registry Information	
URI	The SIP URI that is trying to register. (This field only indicates that a SIP device tried to register, not that it succeeded.)
Local IP Address	The local, LAN IP address of the SIP device.
Expiration	Indicates how long (in seconds) until the registration expires.

## 16. NAT SERVICES

For your convenience, VersaLink supports protocols for Applications, Games, and VPN-specific programs. The following chart provides protocol information for the services supported by VersaLink.

NOTE: To configure VersaLink for a service or application, follow the steps in section 13 (Setting Up Advanced Service Configuration) of this User Guide.

**Applications/Games/VPN Support**

Application/Game	Port/Protocol
Aliens vs. Predator	80 UDP, 2300 UDP, 8000-8999 UDP
America Online	5190 TCP/UDP
AoE II: Conquors	47624 TCP/UDP, 6073 TCP/UDP, 2300-2400 TCP/UDP
AOL Instant Messenger	4099 TCP, 5190 TCP
Asheron's Call	9000-9013 UDP, 28800-29000 TCP
Battlecom	2300-2400 TCP/UDP, 47624 TCP/UDP
Black and White	2611-2612 TCP, 6667 TCP, 6500 UDP, 27900 UDP
Blizzard Battle.net (Diablo II)	4000 TCP, 6112 TCP/UDP
Buddy Phone	700, 701 UDP
Bungie.net, Myth, Myth II Server	3453 TCP
Calista IP Phone	3000 UDP, 5190 TCP
Citrix Metaframe	1494 TCP
Client POP/IMAP	110 TCP
Client SMTP	25 TCP
Counter Strike	27015 TCP/UDP, 27016 TCP/UDP
Dark Reign 2	26214 TCP/UDP
Delta Force ( Client and Server )	3568 UDP, 3100-3999 TCP/UDP
Delta Force 2	3568-3569 UDP
DeltaForce: Land Warrior	UDP 53 TCP 21 TCP 7430 TCP 80 UDP 1029 UDP 1144 UDP 65436 UDP 17478
DNS	53 UDP
Elite Force	2600 UDP, 27500 UDP, 27910 UDP, 27960 UDP
Everquest	1024-7000 TCP/UDP
F-16, Mig 29	3863 UDP
F-22 Lightning 3	4660-4670 TCP/UDP, 3875 UDP, 4533-4534 UDP, 4660-4670 UDP
F-22 Raptor	3874-3875 UDP
Fighter Ace II	50000-50100 TCP/UDP
Fighter Ace II for DX play	50000-50100 TCP/UDP, 47624 TCP, 2300-2400 TCP/UDP
FTP	20 TCP, 21 TCP
GameSpy Online	UDP 3783

Application/Game	Port/Protocol
	UDP 6515 TCP 6667 UDP 12203 TCP/UDP 13139 UDP 27900 UDP 28900 UDP 29900 UDP 29901
Ghost Recon	TCP 80 UDP 1038 UDP 1032 UDP 53 UDP 2347 UDP 2346
GNUTella	6346 TCP/UDP, 1214 TCP
Half Life Server	27005 UDP(client only) 27015 UDP
Heretic II Server	28910 TCP
Hexen II	26900 (+1) each player needs their own port. Increment by one for each person
Hotline Server	5500, 5503 TCP 5499 UDP
HTTPS	443 TCP/UDP
ICMP Echo	4 ICMP
ICQ OLD	4000 UDP, 20000-20019 TCP
ICQ 2001b	4099 TCP, 5190 TCP
ICUII Client	2000-2038 TCP, 2050-2051 TCP, 2069 TCP, 2085 TCP, 3010-3030 TCP
ICUII Client Version 4.xx	1024-5000 TCP, 2050-2051 TCP, 2069 TCP, 2085 TCP, 3010-3030 TCP, 2000-2038 TCP 6700-6702 TCP, 6880 TCP, 1200-16090 TCP
IMAP	119 TCP/UDP
IMAP v.3	220 TCP/UDP
Internet Phone	22555 UDP
IPSEC ESP	PROTOCOL 50
IPSEC IKE	500 UDP
Ivisit	9943 UDP, 56768 UDP
KALI, Doom & Doom II	2213 UDP, 6666 UDP (EACH PC USING KALI MUST USE A DIFFERENT PORT NUMBER STARTING WITH 2213 + 1
KaZaA	1214 TCP/UDP
Limewire	6346 TCP/UDP, 1214 TCP
Medal Of Honor: Allied Assault	TCP 80 UDP 53 UDP 2093 UDP 12201 TCP 12300 UDP 2135 UDP 2139 TCP/UDP 28900

Application/Game	Port/Protocol
mIRC Chat	6660-6669 TCP
Motorhead Server	16000 TCP/UDP, 16010-16030 TCP/UDP
MSN Game Zone	6667 TCP, 28800-29000 TCP
MSN Game Zone (DX 7 & 8 play)	6667 TCP, 6073 TCP, 28800-29000 TCP, 47624 TCP, 2300-2400 TCP/UDP
MSN Messenger	6891-6900 TCP, 1863 TCP/UDP, 5190 UDP, 6901 TCP/UDP
Napster	6699 TCP
Need for Speed 3, Hot Pursuit	1030 TCP
Need for Speed, Porsche	9442 UDP
Net2Phone	6801 UDP
NNTP	119 TCP/UDP
Operation FlashPoint	47624 UDP, 6073 UDP, 2300-2400 TCP/UDP, 2234 TCP
Outlaws	5310 TCP/UDP
Pal Talk	2090-2091 TCP/UDP, 2095 TCP, 5001 TCP, 8200-8700 TCP/UDP, 1025-2500 UDP
pcAnywhere host	5631 TCP, 5632 UDP, 22 UDP
Phone Free	1034-1035 TCP/UDP, 9900-9901 UDP, 2644 TCP, 8000 TCP
Quake 2	27910 UDP
Quake 3	27660 UDP Each computer playing QuakeIII must use a different port number, starting at 27660 and incrementing by 1. You'll also need to do the following: 1. Right click on the QIII icon 2. Choose "Properties" 3. In the Target field you'll see a line like "C:\Program Files\Quake III Arena\quake3.exe" 4. Add the Quake III net_port command to specify a unique communication port for each system. The complete field should look like this: "C:\Program Files\Quake III Arena\quake3.exe" +set net_port 27660 5. Click OK. 6. Repeat for each system behind the NAT, adding one to the net_port selected (27660,27661,27662)
Quicktime 4/Real Audio	6970-32000 UDP, 554 TCP/UDP
Rainbow Six & Rogue Spear	2346 TCP
RealOne Player	TCP - 554, 7070 to 7071 UDP - 6970 to 7170
Real Audio	6970-7170 UDP
Roger Wilco	TCP/UDP 3782 UDP 3783 (BaseStation)
ShoutCast Server	8000-8005 TCP
SSH Secure Shell	22 TCP/UDP
Starcraft	2346 TCP
Starfleet Command	2300-2400 TCP/UDP, 47624 TCP/UDP
Telnet	23 TCP
Tiberian Sun & Dune 2000	1140-1234, 4000 TCP/UDP
Ultima Online	5001-5010 TCP, 7775-7777 TCP, 8800-8900 TCP, 9999 UDP, 7875 UDP

<b>Application/Game</b>	<b>Port/Protocol</b>
Unreal Tournament server	7777 (default gameplay port) 7778 (server query port) 7779,7779+ are allocated dynamically for each helper UdpLink objects, including UdpServerUplink objects. Try starting with 7779-7781 and add ports if needed 27900 server query, if master server uplink is enabled. Home master servers use other ports like 27500 Port 8080 is for UT Server Admin. In the [UWeb.WebServer] section of the server.ini file, set the ListenPort to 8080 and ServerName to the IP assigned to VersaLink from your ISP.
USENET News Service	143 TCP
VNC, Virtual Network Computing	5500 TCP, 5800 TCP, 5900 TCP
Westwood Online, C&C	4000 TCP/UDP, 1140-1234 TCP/UDP
World Wide Web (HTTP)	80 TCP 443 TCP (SSL) 8008 OR 8080 TCP (PROXY)
XBOX Live	TCP/UDP 88 and 3074
Yahoo Messenger Chat	5000-5001 TCP
Yahoo Messenger Phone	5055 UDP
<b>VPN Protocol</b>	<b>Comments</b>
IPSec Encryption	IPSec using AH can not be supported through NAT. IPSec using ESP and L2TP can be supported via an ALG
L2TP	IPSec using ESP and L2TP can be supported via an ALG.
PPTP	Works through NAT.

## 17. HELP

If you select **Help** from the menu bar, a message from the help screens will be displayed. The type of message displayed depends on the menu that you are viewing. If you are viewing a pop-up screen, click the **help** link in the pop-up screen to obtain help messages.

# A

## About

This screen provides information about VersaLink. The following settings are displayed.

About	
Model Number	VersaLink manufacturer's model number.
Serial Number	VersaLink manufacturer's serial number.
MAC Address	Ethernet MAC (i.e., hardware) Address of VersaLink.
Software Version	VersaLink application software version number.
Software Model	VersaLink application type.
Description	Description of VersaLink protocol processing application software.
Boot Loader	VersaLinks boot loader version number.

## Advanced Home Page

The advanced home page offers the same functionality as the home page but adds the ability to change the connection profile settings defined in VersaLink.

About	
Edit	An "Edit" link is added for each connection profile. Selecting this link will pop up a window that allows the connection profile settings to be changed.
New Connection	The "New Connection" link will pop up a window to allow the creation of a new connection profile.

## ATM Loopback

ATM Loopback	
ATM Loopback	This setting enables 0/21 loopback. Westell recommends that you <u>do not</u> change this setting.

## B

### Backup/Restore

This option allows VersaLink configuration to be backed up to or restored from a secure location in flash. The following options are displayed.

Backup/Restore	
Current becomes Back-up	Selecting this command button will backup the current active configuration to the secure flash location.
Back-up becomes Current	This command button will restore the previously stored configuration from the flash location.
Factory becomes Current	This option will restore VersaLink to the state that it arrived in from the factory.

## C

### Change Administration Password

VersaLink has an administrator password. This password protects VersaLink from any unauthorized modifications to the configuration setting in VersaLink. The following settings are displayed.

Change Administration Password	
Enter Administration Name	This field specifies the Administrator's name. Only one administrator can be defined.
Enter/Verify Administration Password	This field specifies the password required to enable administrator access. The password must be entered twice to ensure that the password has been entered correctly.

### Connection Summary

Connection Summary	
Connection Summary	The connection profile screen displays summary information about VersaLink. The connection state is shown along with the amount of traffic has passed through VersaLink. Each connection profile is listed with its associated usage information.

# D

## Diagnostics Help

This screen provides tools for diagnosing PPP connection problems. Some tests depend on VersaLink's status and the capabilities exercised by previous tests, which may prevent other types of testing.

### *Beginning of Diagnostics Help screens*

#### **DSL**

VersaLink status checks the connection. The following is a list of the possible responses:

<b>DSL</b>	
Up	VersaLink is operating correctly and has obtained synchronization with the opposing DSLAM.
Down	Explanation: VersaLink is operating correctly, but has not synchronized with the opposing DSLAM. Solution: First, check to be sure that the cable connecting VersaLink to the ADSL wall jack is properly connected at both ends. If the cable is properly connected and VersaLink does not synchronize, try another phone cable. Next, wait for VersaLink to train. It can sometimes take as long as two minutes for VersaLink to train. If it still has not come into synchronization, power cycle VersaLink. If you have tried the approach above and VersaLink still does not synchronize, contact your service provider.

#### **PPPoE**

The PPPoE status indicates if a PPPoE session is established (i.e., if the PPPoE Discovery procedure has completed). The following is a list of the possible responses:

<b>PPPoE</b>	
Session up	A valid PPPoE session has been detected.
no session	Currently there is no active PPPoE session. A PPP session must be connected from the homepage screen.
initiating session	The connection process for a PPPoE session has been initialized. It can sometimes take a few seconds for the PPPoE Discovery procedure to complete. Wait 10-15 seconds and try again. If the PPPoE Discovery still cannot complete, there may be a configuration issue with your service provider's equipment. Verify your VPI/VCI settings (on the LAN Advanced page) and contact your ISP provider.
Session halted	A successful PPPoE session was halted. A PPP session must be connected from the homepage screen.
passed	A valid PPPoE session was established.
Session failure	A PPPoE session could not be made. There may be a configuration issue with your service provider's equipment. Verify your VPI/VCI settings (on the LAN Advanced page) and contact your provider.

## PPP

This field displays the PPP Connection status. A PPPoE or PPPoA session must already be established. The following is a list of the possible responses:

PPP	
Connection up	VersaLink has established a PPP connection.
no connection	There is no PPP connection. A PPP session must be connected from the homepage screen.
initiating connection	The PPP connection process has been initialized.
Connection halted	A successful PPP connection was halted. Solution: A PPP session must be connected from the homepage screen.
Cannot connect	Explanation: A PPP connection could not be made because of a PPPoE session failure.
Authorization failure	The username or password is incorrect. Verify that the username and password your Service Provider issued are entered correctly.
Link control protocol failed	Try re-establishing the session (from the home page). If this doesn't help, there may be a configuration issue or other failure with your provider's equipment. Contact your service provider.

## Self Test

The Self Test performs an integrity check of certain internal components of VersaLink. The following is a list of the possible responses:

Self Test	
<b>Success</b>	VersaLink is operating correctly.
Flash Corrupt	Explanation: The self-test process has detected a problem with internal flash memory. Solution: Restart VersaLink. If the error persists, contact your service provider.

## PING ISPs' VersaLink

The IP remote VersaLink test performs an IP network check (i.e., an IP Ping) of the Service Provider's VersaLink. This test verifies that VersaLink can exchange IP traffic with an entity on the other side of the DSL line. The following is a list of the possible responses:

PING ISP's VersaLink	
Success	VersaLink has detected an IP remote VersaLink connection.
No Response	Explanation: This message will occur when an IP remote VersaLink does not answer the IP Ping. Solution: This test fails when the provider's VersaLink does not give its IP address to VersaLink during session establishment. Try Pinging another host, using the Ping test near the bottom of the Diagnostic screen. If you are able to Ping any host, or even if you are able to find an IP address for a given host name (try "www.yahoo.com"), then the failure of the "IP Remote VersaLink" test is moot, because the success of the Ping demonstrates that you are getting IP traffic across the DSL line. If the separate Ping fails as well, contact your service provider.
could not test	Explanation: Test could not be executed because of VersaLink status.

## DNS

The DNS test issues a request to try to resolve the name of a particular host. The host name is entered in the input box. The following is a list of the possible responses:

<b>DNS</b>	
Success	VersaLink has successfully obtained the resolved address. The IP address is shown below the host name input box
No Response	Explanation: VersaLink has failed to successfully obtain the resolved address. Solution: Determine the IP addresses of your DNS servers (from the home page, click "Edit" and then "Advanced"), and then use the Ping test near the bottom of the Diagnostic screen to try to Ping those addresses. This may provide useful information when you contact your service provider and speak with Technical Support.
Host not found	Explanation: The DNS Server was unable to find an address for the given host name. Solution: That host may no longer be available on the Internet. Try entering a different host name.
No data, enter host name	Explanation: There must be a host name entered in the input box.
could not test	Explanation: Test could not be executed because of VersaLink status.

## PING

Select **PING** to check IP continuity to a remote computer either within or beyond the Service Providers network.

Enter either the IP address or the hostname of the remote host computer into the input box to the right of the Test button. If you Ping by name, DNS will be used to look up the appropriate IP address for that name.

The following is a list of the possible responses:

<b>PING</b>	
Success	The Remote Host Computer was detected.
No Response	Explanation: This message will occur when there was no response to the Ping from the remote computer. Solution: Bear in mind that many hosts on the Internet are configured for security reasons to not respond to IP Ping messages. If you get a success from the DNS test using the same host name, chances are good that your connection is fine, whether you can Ping the named host or not.
No name or address to PING	Explanation: There must be a host name or IP address entered in the input box to allow VersaLink to Ping.
could not test	Explanation: Test could not be executed because of VersaLink status.

## *End of Diagnostic Help Screens*

## DHCP Configuration

This screen contains the settings which control how VersaLink interacts with the local devices connected to VersaLink. Westell does not recommend that you change these settings. The following settings are displayed.

DHCP	
DHCP Server	Dynamic Host Configuration Protocol (DHCP) is an Internet standard that allows VersaLink to automatically assign IP addresses to devices connected on the LAN network. It is advised that this is enabled for Private LAN.
DHCP Start Address (If DHCP is enabled)	This setting specifies the start of the IP address pool that the modem uses to assign IP addresses to local devices.
DHCP End Address (If DHCP is enabled)	This setting specifies the end address of the IP address pool used for automatic configuration of local devices.
DHCP Lease (If DHCP is enabled)	This setting specifies the DHCP lease time.

## Diagnostic Log

LOGS	
All	Lists both connection and system logs.
Connection	Lists all events related to connection activity (Any traffic on the USB, Ethernet, or DSL ports).
System	Lists all events related to system activity (Time, Errors, Boot Information, etc.).
Remote Logging	
Remote Logging	Contains the configuration for the diagnostics remote logging. Remote diagnostics logging allows the diagnostics logs to be sent to a machine running a syslog server*. If you want to save the diagnostics logs, remote diagnostics logging should be enabled and the IP address of the syslog server must be configured.
Enable	Enables remote logging of diagnostics logs.
Remote IP Address	The IP address of the syslog server machine to which the diagnostics log are to be sent.
*The syslog server must be configured to listen on udp port 514, which is usually the default port. In order for the logs to be saved to the syslog server, the server should be configured to save the logs to a file. Some of the free syslog servers available on the Internet are kiwisyslog, MT syslog and 3Csyslog.	

## DNS Configuration

VersaLink has a built-in DNS server. VersaLink has a feature called "Dynamic DNS." When an IP address is assigned, VersaLink will interrogate the new device for a machine name using several well-known networking protocols. Any names learned will dynamically be added to the DNS server's table of local hosts. A static host assignment is needed only if the new device does not support any of the well-known protocols. The following settings are displayed.

DNS Configuration Screen	
Domain Name	The name of your network. This uses the internet standard for delineating domain names.
Static Host Assignment	This table allows the creation and maintenance of manually configured DNS entries.
Dynamic Host Assignment	This table shows the current list of devices that have automatically provided information.

# E

## Edit Connection Profiles

This screen facilitates the changing of connection profile parameters. The following settings are displayed.

Edit Connection Profiles	
Connection Name	This field is a description of the default connection profile that VersaLink will use. Feel free to use whatever description you desire.
Account ID	Your account ID is supplied by your ISP. This text string uniquely identifies you with your ISP.
Account Password	The Account Password is a key phrase or text string that verifies your identity to the ISP.
Service Profile	VersaLink stores several service profiles. A service profile is a collection of settings for the built-in firewall and NAT. These settings control which applications are enabled to talk through VersaLink. This selection specifies which service profile is used when VersaLink is using this connection.
Manual/Auto/Always ON	These radio buttons specify how this connection profile is used. A manual setting requires that this connection must be manually established through the “homepage” connection button. When this is set to auto, VersaLink will monitor the network traffic and determine when a connection needs to be made. The connection process will happen automatically the “Always ON” selection causes VersaLink to aggressively establish a connection with your ISP. Whenever VersaLink detects that the connection to your ISP is down, it will try to re-establish that connection.
Time Out Enable/Connection Time Out	Selecting this option will enable the disconnect timeout. If this option is enabled VersaLink will monitor the ISP connection for activity. If there is no activity for the timeout period, VersaLink will disconnect from the ISP.
Edit VC Connection	This screen is an advanced screen. Modifying parameters identified on this screen can cause severe disruption of your service. VC stands for “Virtual Connection.” A VC identifies a connection through the service provider’s ATM network to your ISP. It is not recommended that you change anything on these pages unless explicitly instructed by your service provider.

# F

## Firewall Log

This screen is an advanced diagnostics screen. It alerts you of noteworthy information sent to your modem from the Internet. One thousand entries can be made, but a maximum of 50 entries are displayed at a time. Once 1000 entries have been logged, the oldest entry is removed to make space for new entries as they occur.

Firewall Log	
Details	This option gives more information about the specific log entry
Page Numbers	This option navigates you to the corresponding range of entries. The most recent entries are always on the highest numbered page.
Clear Log	This option removes all entries from the log.
Print/Savable Format	This option opens a new window that contains a list of all logged packets that can be saved or printed.

## Firewall Settings

This screen is an advanced configuration screen. It allows you to set the level of security you wish to have on your local network. All security levels except “None” protect against known Internet attacks and devices that attempt to gain remote access to VersaLink. The following settings are displayed.

Firewall Settings	
High	This security level only allows basic Internet functionality. Only Mail, News, Web, FTP, and IPSEC are allowed. No other traffic is allowed. Another restriction of high security is that it can't be modified by NAT configuration options. With High security, you are guaranteed to only pass the previously mentioned traffic.
Medium	This security level only allows basic Internet functionality by default, just like High security. Medium security, however, allows Customization through NAT configuration, so you can enable the traffic that you want to pass.
Low	The low security setting will allow all traffic except for known attacks. With low security, your Gateway is visible by other computers on the Internet.
Custom	Custom is a very advanced configuration option that allows you to edit the firewall configuration directly. Only the most expert users should try this.
Remote Logging	Contains the configuration for the firewall remote logging. Remote firewall logging allows the firewall logs to be sent to a machine running a syslog server*. If you desire to save the firewall logs, remote firewall logging must be enabled and the IP address of the syslog server must be configured.
Enable	This option enables remote logging of firewall logs.
Remote IP Address	The IP address of the syslog server machine on the local area network to which the firewall logs are to be sent.
*The syslog server must be configured to listen on udp port 514, which is usually the default port. In order for the logs to be saved to the syslog server, the server should be configured to save the logs to a file. Some of the free syslog servers available on the Internet are kiwisyslog, MT_syslog and 3Csyslog.	

# H

## Home Page

The home page gives you a quick summary of VersaLink's state. The following settings are displayed.

Home Page	
Connection Overview	The Connection Overview section displays the status of the DSL connection. The DSL must show a state of “UP” to allow VersaLink to communicate with your service provider's network.
Connection Name	The Connection Name section displays all of the connection profiles that are defined by VersaLink. A connection profile is information that VersaLink needs to establish a connection to your ISP. The “PPP Status” columns will show a status of “UP” if VersaLink is currently using that profile to communicate. The command button allows you to control the connection state.
Profile Editor	Selecting the “Profile Editor” link will allow you to define or change any of the connection profile settings.

# L

## LAN Configuration

This screen contains the setting that controls how VersaLink interacts with the local devices connected to VersaLink. Westell does not recommend that you change these settings. The following settings are displayed.

LAN Configuration	
Gateway IP Address	This controls the IP address that VersaLink uses for local communication.
Subnet Mask	This setting specifies the subnet mask to use to determine if an IP address belongs to your local network.
DHCP Start Address	This setting specifies the start of the IP address pool that VersaLink uses to assign IP addresses to local devices.
DHCP End Address	This setting specifies the end address of the IP address pool used for automatic configuration of local devices.
DNS Server Enable	DNS stands for Domain Name System. This is an Internet standard that facilitates communication among devices. This allows a name to be used when specifying a device instead of an IP address. Normally you want this enabled.
DHCP Server Enable	DHCP stands for Dynamic Host Configuration Protocol. This is an Internet standard that allows VersaLink to automatically assign IP addresses to devices connected on the LAN network. It is advised that this option is set to Enabled.

## LAN Statistics

This page contains information regarding the configuration and status of your Local LAN. The following settings are displayed.

LAN Configuration	
Device IP Address	This displays the IP address that VersaLink uses for local communication.
DHCP NetMask	This displays the subnet address that VersaLink's DHCP server issues in DHCP responses.
DHCP Start Address	This setting specifies the start of the IP address pool that the modem uses to assign IP addresses to local devices.
DHCP End Address	This setting specifies the end address of the IP address pool used for automatic configuration of local devices.
DHCP Server Status	Displays the status, "ON" or "OFF" of the DHCP Server
DHCP Server	Displays which network "Public" or "Private" the DHCP server is serving IP addresses for.
Devices on LAN	This page displays the current devices the modem has found on your LAN. The name of the device, the Ethernet MAC address, and the status, "Active" or "Inactive" is displayed in the table.

# P

## Private LAN

This page contains the settings that control how VersaLink interacts with the local devices connected to VersaLink. It is not recommended that these settings be changed. The following settings are displayed.

Private LAN	
Private LAN DHCP Server Enable	Dynamic Host Configuration Protocol (DHCP) is an Internet standard that allows VersaLink to automatically assign IP addresses to devices connected on the LAN network. It is advised that this is enabled for Private LAN.
Private LAN Enable	This setting enables the Private NAT'ed interface. It is advised to leave this enabled.
Modem IP Address	This controls the IP address that VersaLink uses for local communication.
Subnet Mask	This setting specifies the subnet mask to use to determine if an IP address belongs to your local network.
DHCP Start Address (If DHCP is enabled for Private LAN)	This setting specifies the start of the IP address pool that the modem uses to assign IP addresses to local devices.
DHCP End Address (If DHCP is enabled for Private LAN)	This setting specifies the end address of the IP address pool used for automatic configuration of local devices.
DHCP Lease (If DHCP is enabled for Private LAN)	This setting specifies the DHCP lease time.

## Protocol

Protocol	
Protocol	This screen informs VersaLink which networking protocol to use when communicating with your ISP. This information is provided by your ISP.

## Public LAN

This screen contains the settings that control how VersaLink interacts with the local devices connected to VersaLink. It is not recommended that these settings be changed. The following settings are displayed.

Public LAN	
Public LAN DHCP Server Enable	Dynamic Host Configuration Protocol (DHCP) is an Internet standard that allows VersaLink to automatically assign IP addresses to devices connected on the LAN network. It is advised that this is enabled for Private LAN.
Public LAN Enable	This setting enables the Public interface. This feature allows a global subnet to exist behind your modem.
Modem IP Address	This controls the IP address that VersaLink uses for local communication.
Subnet Mask	This setting specifies the subnet mask to use to determine if an IP address belongs to your local network.
DHCP Start Address (If DHCP is enabled for Public LAN)	This setting specifies the start of the IP address pool that the modem uses to assign IP addresses to local devices.
DHCP End Address (If DHCP is enabled for Public LAN)	This setting specifies the end address of the IP address pool used for automatic configuration of local devices.



Public LAN)	
DHCP Lease (If DHCP is enabled for Public LAN)	This setting specifies the DHCP lease time.

## Q

### Quality of Service

Quality of Service	
Quality of Service	This feature helps ensure data integrity in high-speed transmissions. This feature provides the capability to partition network traffic into multiple priority levels or classes of service. After packet classification, other QoS fetures can be utilized to assign the appropriate traffic handling policies including congestion management, bandwidth allocation, and delay bounds for each traffic class.

## R

### Remote Access

This page allows you to configure your modem so that it can be configured remotely. Once enabled, this feature can be manually disabled, or it will automatically disable after 20 minutes of configuration inactivity.

Remote Access	
Password	This is the password a remote user must enter to access your modem's interface. It must be at least 4 characters long and contain no spaces.
URL	This field contains the URL that must be placed in a remote PC's web browser in order to communicate with your modem. If this field says "Not Connected," you are not currently connected to the Internet.
Enable Remote Access	When you have clicked on this button, entered a valid password, and connected to the Internet, Remote Access will be enabled.
Disable Remote Access	When you have clicked on this button, Remote Access will be disabled.

### Routing Information Protocol

Remote Access	
RIP	RIP (Routing Information Protocol) is a widely used protocol for managing VersaLink information within a self-contained network such as a corporate local area network or an interconnected group of such LANs.

# S

## Single Static IP

This page contains the settings that would allow the PPP address received from the network to be propagated to a single LAN device behind the modem.

Single Static IP	
WAN IP Address	This is the PPP IP address the ISP has assigned the modem.
Selection box	<p>This box contains the devices available to share the Single Static IP address the ISP has assigned the modem. The names listed in the select box will be populated by VersaLink's DHCP server based on DHCP requests. If a device's name cannot be determined, the current IP address of the device will be placed in the list.</p> <p>When the feature is enabled, the active machine will be highlighted in the select box and be displayed at the bottom of the page with the "disable" button.</p> <p>When the feature is disabled, no device in the select box will be highlighted and the "enable" button will be available.</p> <p>When the "User Configured PC" is selected, a local PC must be configured manually with the WAN IP address as its Ethernet adapter's address.</p>

# T

## Trace Route

The Trace feature allows you to perform an IP trace route to a remote computer either within or beyond the Internet service provider's network. Enter either the IP address or the hostname of the remote host computer into the input box to the right of the Trace button. If you trace by name, DNS will be used to look up the appropriate IP address for that name.

Trace	
Success	Trace will display its progress in the text box. Trace will show three round trip times and the DNS name (if available) of each intermediate VersaLink.
Failure	Trace will display "*" when it does not receive a response or cannot determine the DNS name of an intermediate Gateway. This is not necessarily an error, as some Gateways are configured to ignore trace route packets or do not have DNS name.

## Turbo TCP

Turbo	
<p>Turbo TCP is a sophisticated network traffic prioritization and queuing method that dramatically improves the performance of downstream TCP/FTP/HTTP transfers under heavy upstream bandwidth utilization conditions.</p> <p>This feature first assigns a high priority to TCP signaling packets in the upstream direction, then places the packet in one of several transmit queues based on this priority.</p> <p>Packets of unspecified priority, like TCP or UDP data, are assigned a low priority and placed in a low priority queue.</p> <p>The packets in the high priority queues are then transmitted before packets in the lower priority queues minimizing any transmit delays.</p> <p>Minimizing the transmit delay of the TCP messages upstream enables the server to send the TCP data downstream faster, resulting in a substantial throughput gain.</p>	

## U

### Update Device

Update Device (Software Upgrade)	
Update Device (Software Upgrade)	This screen is used to upgrade VersaLink's application image. The application image is specified by entering in the filename or by using the browse button.

### User Name

This screen is asks for information that will allow VersaLink to make a connection to the ISP on your behalf. VersaLink will need to know your Account ID and Account Password. This information is stored in VersaLink.

User Name	
Connection Name	This is a description of the default connection profile, which VersaLink will use. Feel free to use whatever description you desire.
Account ID	Your Account Id is supplied by your ISP and is a text string that uniquely identifies you with your ISP.
Account Password	The Account Password is a key phrase or text string that verifies your identify to the ISP.

## V

### VC Configuration

VC Configuration Screen	
VC Configuration	This screen is an advanced screen. Modifying parameters on this screen can cause severe disruption of your service. VC stands for "Virtual Connection." A VC identifies a connection through the service provider's ATM network to your ISP. It is not recommended that anything be changed on these pages unless explicitly instructed by your service provider.

## VLAN

VC Configuration Screen	
VLAN	A virtual (or logical) LAN is a local area network with a definition that maps workstations on some other basis than geographic location.

## VPI/VCI

VPI/VCI	
VPI/VCI	This screen asks for information that VersaLink needs to establish a communication channel to your ISP. The VPI and VCI values are supplied by your ISP.

# W

## Wireless Configuration

<b>ACRONYMS</b>	AP-Access Point BSSID-Basic Service Set ID FW-Firmware MAC-Media Access Controller NIC-Network Interface Card PBCC-Packet Binary Convolutional Code SSID-Service Set ID WEP-Wired Equivalent Privacy WLAN-Wireless Local Area Network
<b>Network Name (SSID)</b>	This string, (32 characters or less) is the name associated with the AP. To connect to the AP, the SSID on a Station card must match the SSID on the AP card or be set to "ANY."
<b>Channel</b>	The AP transmits and receives data on this channel. The number of channels to choose from is pre-programmed into the AP card. Station cards do not have to be set to the same channel as the AP; the Stations scan all channels, and look for an AP to connect to.
<b>WEP Security</b> <b>WEP (Wired Equivalent Privacy)</b>	The AP card supports 64-bit, 128-bit, or 256-bit WEP encryption. The WEP option can also be disabled. If so, any station can connect to the AP (as long as its SSID matches the AP SSID).
<b>text only WEP Key</b>	If selected, the WEP Key is treated as a string of text characters, and the number of characters must be either 5 (for 64-bit encryption) or 13 (for 128-bit encryption) or 29 (for 256-bit encryption). If not selected, the WEP key is treated as a string of hexadecimal characters, and the number of characters must be either 10 (for 64-bit encryption), 26 (for 128-bit encryption), or 58 (for 256-bit encryption). The only allowable hexadecimal characters are 0-9 and A-F. NOTE: The WEP key must be the same value and type for both VersaLink and the wireless network adapter. "Pass Phrase" is not the same as "text" and should not be used.
<b>Enhanced Security</b>	If selected, the SSID is hidden from detection in certain frames of the radio protocol. This makes the SSID harder to discover by external equipment capable of passively scanning the radio signal. Additionally, the station SSID must match the AP Network Name (SSID); the generic station SSID, "ANY"

	will be refused.
<b>Data Rates (Mbits/s)</b>	These are the allowable communication rates that the AP will attempt to use. The rates are broadcast within the connection protocol as rates supported by the VersaLink. If multiple rates are chosen, multi-rate communication and automatic optimum rate selection is possible. This is the default, and provides the most flexible system. If the Station signal strength or quality is poor, and the throughput of the connection is slow or intermittent, select only the lower two data rates (1 and 2 MB). This can improve performance by reducing the number of pad packets, re-tries and timeouts that could be occurring when the higher rates are automatically trying to be used. Lower rates can be maintained over longer distances and in a wider range of environments.

## Wireless Station Configuration

The configuration of wireless stations must correspond with VersaLink's configuration. Typically, WLAN station cards come with a utility for changing the card configuration. Additionally, the WLAN driver might present configuration options as part of the Properties for the installed wireless network adapter. The following configuration items should be considered when setting up a station card.

<b>SSID</b>	This is a description of the default connection profile, which VersaLink will use. Feel free to use whatever description you desire.
<b>Mode</b>	The station's operating mode must be set to, Infrastructure. Most station configuration software will use this term to indicate operation with an AP. Other terms used are ESS or BSS. The terms Ad-Hoc or IBSS indicate operation without an AP; these terms should not be selected.
<b>Tx Rate (Data Rate)</b>	The station's transmission rate (data rate) should be set to Automatic. Selecting a specific data rate is typically only done in difficult environments where conditions limit the maximum possible rate to less than 54 megabits per second.
<b>Encryption</b>	The station's encryption settings must match the AP's settings. This includes the settings for 64-bit, 128-bit, and 256-bit encryption (or none) and the WEP keys. Make certain that the key entries use the same format. The two typical formats provided are simple text entry and hexadecimal entry. Text entry is sometimes termed ASCII entry. <b>Hexadecimal entry is sometimes termed Hex or Manual entry. Do not use the Pass Phrase option if it is present.</b>
<b>Authentication Algorithm</b>	On the station, this setting is typically located under the Advanced properties for the wireless network adapter. Two or three algorithm settings are usually present. These might be termed: "Must use Shared for WEP," "Automatic based on WEP setting" and/or "WECA compliant." Select "Automatic based on WEP setting" or "Must use Shared for WEP."

## Wireless Statistics

<b>Network Name (SSID)</b>	This string, (32 characters or less) is the name associated with the AP. To connect to the AP, the SSID on a Station card must match the SSID on the AP.
<b>802.11b/g/g+ MAC Address (BSSID)</b>	This is the Media Access Controller address of the AP. It is used as the Basic Service Set Identifier.
<b>Primary FW</b>	Primary firmware version number. This is read from the card and helps determine the AP firmware to use. The format of the number is: ...>. The version number is also needed to identify existing errata.

<b>Secondary FW</b>	Secondary firmware version number. This is the station firmware that the card would use to operate as a wireless station. The format of the number is ...>. The version number is needed to identify existing errata.
<b>OUT and IN</b>	Data preceded by <b>OUT</b> pertain to transmissions from VersaLink to a station; VersaLink is the source. Data preceded by <b>IN</b> pertain to data received by VersaLink; VersaLink is the destination.
<b>OUT-Unicast Frames</b>	The number of successfully transmitted frames whose destination address was a single station, not necessarily the same station, but to any single station: As opposed to a transmission that multiple stations would receive (an example would be a broadcast message).
<b>OUT-Multicast Frames</b>	The number of successfully transmitted frames whose destination address was a multicast address (received by more than one station): not necessarily broadcast to all stations, but more than a single station. Broadcast messages are included in the count.
<b>OUT-Fragments</b>	The number of successful transmissions made. This will typically be greater than the sum of the Unicast and Multicast frames because large frames are broken into multiple transmissions. The number of fragments per frame is based on the Fragmentation Threshold setting (not user-configurable).
<b>OUT-Unicast Bytes</b>	The number of bytes transmitted in Unicast Frames. This includes the header and body of each frame.
<b>OUT-Multicast Bytes</b>	The number of bytes transmitted in Multicast Frames. This includes the header and body of each frame or frame fragment.
<b>OUT-Transmission Deferred</b>	The number of frames (frame fragments) for which one or more transmission attempts were deferred to avoid a collision.
<b>OUT-Frames after single retry</b>	The number of frames that were successfully transmitted after one, and only one, retry. All fragments of the frame must have met this requirement if the frame was fragmented.
<b>Wireless Statistics Cont.</b>	
<b>OUT-Frames after many retries</b>	The number of frames that successfully transmitted after more than one retry. Any fragment of a frame that required multiple retries would increment this counter for the whole frame.
<b>OUT-Dropped Frames, too many retries</b>	The number of frames that did not transmit due to the short or long retry limit being reached. This number is a result of no acknowledgement or CTS received.
<b>OUT-Discarded Frames</b>	The number of transmit requests that were discarded to free up buffer space. This count is incremented when one of the following occurs: 1) A transmit request is queued too long on the transmit queue due to excessive retries, deferrals, scans, etc. 2) A transmit request is queued too long on the Power-Save queue because the station did not poll or wake up in time.
<b>IN-Unicast Frames</b>	The number of successfully received frames whose destination address was a single location, not necessarily the same location, but to any single location (as opposed to the broadcast address).
<b>IN-Multicast Frames</b>	The number of successfully received frames whose destination address was a multicast address. Broadcast messages are included in this count.
<b>IN-Fragments</b>	The number of fragments successfully received. This might not be equal to the sum of the Unicast and Multicast frames because large frames are broken into multiple transmissions. The number of fragments per frame is based on the Fragmentation Threshold setting (not user-configurable) on the source station.
<b>IN-Unicast Bytes</b>	The number of bytes received in Unicast Frames. This includes the header and body of each frame or frame fragment.
<b>IN-Multicast Bytes</b>	The number of bytes received in Multicast Frames. This includes the header and body of each frame or frame fragment.

<b>IN-Packet not passing checksum</b>	The number of received frames with a Frame Check Sequence (FCS) error.
<b>IN-Drops due to insufficient Rx buffers</b>	The number of received frames discarded due to lack of buffer space.
<b>IN-Un-decryptable packets</b>	The number of received frames (with the WEP sub-field set to one) that were discarded because the frame should not have been encrypted or the source station did not have privacy enabled.
<b>IN-Messages received in message fragments</b>	The number of frames received successfully while another good reception was going on above the carrier detect threshold (the message-in-message path #1 in the modem).
<b>IN-Messages received in bad message fragments</b>	The number of frames received successfully while another reception was going on above the carrier detect threshold, but with a bad or incomplete PLCP Preamble and Header (the message-in-message path #2 in the modem).



WESTELL

User Guide

VersaLink™ Gateway

## 18. TECHNICAL SUPPORT INFORMATION

### Westell Technical Support

If technical assistance is required, contact Westell by using one of the following options:

North America

Phone: 1-630-375-4900

U.K./Europe

Phone: (44) 01256 843311

Visit Westell at [www.Westell.com](http://www.Westell.com) to view frequently asked questions and enter on-line service requests, or send email to [global\\_support@westell.com](mailto:global_support@westell.com) to obtain additional information.

## 19. WARRANTY AND REPAIRS

### Warranty

Westell warrants this product free from defects at the time of shipment. Westell also warrants this product fully functional for the period specified by the terms of the warranty. Any attempt to repair or modify the equipment by anyone other than an authorized representative will void the warranty.

### Repairs

Westell will repair any defective Westell equipment without cost during the warranty period if the unit is defective for any reason other than abuse, improper use, or improper installation, or acts of nature. Before returning the defective equipment, request a **Return Material Authorization (RMA)** number from Westell. An RMA number must be quoted on all returns. When requesting an RMA, please provide the following information:

- Product model number (on product base)
- Product serial number (on product base)
- Customer ship-to address
- Contact name
- Problem description
- Purchase date

After an RMA number is obtained, return the defective unit, freight prepaid, along with a brief description of the problem to one of the following options:

North America

Westell, Inc.

ATTN: R.G.M Department

750 N. Commons Drive

Aurora, IL 60504-7940 USA

U.K./Europe

Westell, Ltd.

Ringway House

Bell Road

Daneshill

Basingstoke

RG24 8FB

United Kingdom

Westell will continue to repair faulty equipment beyond the warranty period for a nominal charge. Contact a Westell Technical Support Representative for details.

## 20. PRODUCT SPECIFICATIONS

### ADSL

- DSL Line Code: Discrete Multi-Tone (DMT)
- DSL Rates: 32 kbps to 8 Mbps downstream and 32 kbps to 800 kbps upstream
- Power spectral density: less than -34 dBm/Hz
- DSL Impedance: 100 Ohms
- DSL Performance: per ITU Recommendation G.991.2, ANSI T1.413
- Upgradeable to ADSL2, ADSL2+, READSL

### Protocol Features

- Bridge Encapsulation per RFC2684 (Formerly RFC1483)
- Logical Link Control/Subnetwork
- Access Protocol (LLC/SNAP)
- Software Upgradeable
- PPPoE Support
- ATM SAR: Internal to Modem

### System Requirements for 10/100 Base-T/Ethernet

- Pentium® or equivalent and above machines
- Microsoft Windows (95, 98, 2000, ME, NT 4.0, or XP) Macintosh OS X, or Linux installed
- Operating system CD
- Internet Explorer 4.x or Netscape Navigator 4.x or higher
- 64 MB RAM (128 MB recommended)
- Ethernet 10/100 Base-T interface
- 10 MB of free hard drive space
- TCP/IP Protocol stack installed

### System Requirements for Wireless

- Pentium® or equivalent and above class machines
- Microsoft® Windows® (98, 2000, ME, or XP) or Macintosh® OS X installed
- Operating System CD on hand

- Internet Explorer 4.x or Netscape Navigator 4.x or higher
- 64 MB RAM (128 MB recommended)
- 10 MB of free hard drive space
- IEEE 802.11b/g+ PC adapter

### LEDs

- Power
- Ethernet
- Wireless
- DSL
- Internet

### Connectors

- DSL: RJ-11, 6-pin modular jack-DSL
- Ethernet: RJ-45: 8-pin modular jack
- Power: Connector
- SMA antenna

### Power

- Power Supply: External 120 VAC to 9V DC wall-mount power supply
- Power Consumption: Less than 6 watts typical, from 120 VAC

### Environmental

- Ambient Operating Temperature: +32 to +104°F (0 to +40°C)
- Relative Humidity: 5 to 95%, non-condensing

### EMC/Safety/Regulatory Certifications

- EMC: FCC Part 15, Class B
- UL Standard 60950, 3<sup>rd</sup> Edition
- CAN/CSA Standard C22.2 No. 60950
- UL
- CSA
- ACTA 968-A
- Industry Canada CS03

## 21. SOFTWARE LICENSE AGREEMENT

**READ THE TERMS AND CONDITIONS OF THIS LICENSE AGREEMENT CAREFULLY. THIS SOFTWARE IS COPYRIGHTED AND LICENSED (NOT SOLD). BY INSTALLING AND OPERATING THIS PRODUCT, YOU ARE ACCEPTING AND AGREEING TO THE TERMS OF THIS LICENSE AGREEMENT. IF YOU ARE NOT WILLING TO BE BOUND BY THE TERMS OF THIS LICENSE AGREEMENT, YOU SHOULD PROMPTLY RETURN THE SOFTWARE AND HARDWARE TO WESTELL TECHNOLOGIES, INC. THIS LICENSE AGREEMENT REPRESENTS THE ENTIRE AGREEMENT CONCERNING THE SOFTWARE BETWEEN YOU AND WESTELL TECHNOLOGIES, INC. (REFERRED TO AS "LICENSOR"), AND IT SUPERSEDES ANY PRIOR PROPOSAL, REPRESENTATION, OR UNDERSTANDING BETWEEN THE PARTIES.**

**1. License Grant.** Licensor hereby grants to you, and you accept, a nonexclusive license to use the Compact Disk (CD) and the computer programs contained therein in machine-readable, object code form only (collectively referred to as the "SOFTWARE"), and the accompanying User Documentation, only as authorized in this License Agreement. The SOFTWARE may be used only in connection with the number of systems for which you have paid license fees as dictated in your support agreement. You agree that you will not assign, sublicense, transfer, pledge, lease, rent, or share your rights under this License Agreement. You agree that you may not nor allow others to reverse assemble, reverse compile, or otherwise translate the SOFTWARE.

You may retain the SOFTWARE CD for backup purposes only. In addition, you may make one copy of the SOFTWARE in any storage medium for backup purposes only. You may make one copy of the User's Manual for backup purposes only. Any such copies of the SOFTWARE or the User's Manual shall include Licensor's copyright and other proprietary notices. Except as authorized under this paragraph, no copies of the SOFTWARE or any portions thereof may be made by you or any person under your authority or control.

**2. Licensor's Rights.** You acknowledge and agree that the SOFTWARE and the User's Manual are proprietary products of Licensor protected under U.S. copyright law. You further acknowledge and agree that all right, title, and interest in and to the SOFTWARE, including associated intellectual property rights, are and shall remain with Licensor. This License Agreement does not convey to you an interest in or to the SOFTWARE, but only a limited right of use revocable in accordance with the terms of this License Agreement.

**3. License Fees.** The fees paid by you under the support agreement are paid in consideration of the licenses granted under this License Agreement.

**4. Term.** This License Agreement is effective upon your opening of this package and shall continue until terminated. You may terminate this License Agreement at any time by returning the SOFTWARE and all copies thereof and extracts therefrom to Licensor. Licensor may terminate this License Agreement upon the breach by you of any term hereof. Upon such termination by Licensor, you agree to return to Licensor the SOFTWARE and all copies and portions thereof.

**5. Limited Warranty.** Licensor warrants, for your benefit alone, for a period of 90 days from the date of commencement of this License Agreement (referred to as the "Warranty Period") that the SOFTWARE CD in which the SOFTWARE is contained are free from defects in material and workmanship. Licensor further warrants, for your benefit alone, that during the Warranty Period the SOFTWARE shall operate substantially in accordance with the functional specifications in the User's Manual. If during the Warranty Period, a defect in the SOFTWARE appears, you may return the SOFTWARE to Licensor for replacement. You agree that the foregoing constitutes your sole and exclusive remedy for breach by Licensor of any warranties made under this Agreement.



**EXCEPT FOR THE WARRANTIES SET FORTH ABOVE, THE SOFTWARE CD, AND THE SOFTWARE CONTAINED THEREIN, ARE LICENSED "AS IS," AND LICENSOR DISCLAIMS ANY AND ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.**

**6. Limitation of Liability.** Licensor's cumulative liability to you or any other party for any loss or damages resulting from any claims, demands, or actions arising out of or relating to this Agreement shall not exceed the license fee paid to Licensor for the use of the SOFTWARE. In no event shall Licensor be liable for any indirect, incidental, consequential, special, or exemplary damages or lost profits, even if Licensor has been advised of the possibility of such damages. **SOME STATES DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.**

**7. Governing Law.** This License Agreement shall be construed and governed in accordance with the laws of the State of Illinois. You submit to the jurisdiction of the state and federal courts of the state of Illinois and agree that venue is proper in those courts with regard to any litigation arising under this Agreement.

**8. Costs of Litigation.** If any action is brought by either party to this License Agreement against the other party regarding the subject matter hereof, the prevailing party shall be entitled to recover, in addition to any other relief granted, reasonable attorney fees and expenses of litigation.

**9. Severability.** Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, such declaration shall have no effect on the remaining terms hereof.

**10. No Waiver.** The failure of either party to enforce any rights granted hereunder or to take action against the other party in the event of any breach hereunder shall not be deemed a waiver by that party as to subsequent enforcement of rights or subsequent actions in the event of future breaches.



## 22. PUBLICATION INFORMATION

Westell ®VersaLink™ Gateway (Model 327W)  
User Guide Part Number 030-300390 Rev. A  
May 2004

© 2004 Westell, Inc.  
All rights reserved.

Westell, Inc.  
750 North Commons Drive  
Aurora, Illinois 60504 USA  
[www.westell.com](http://www.westell.com)

All trademarks and registered trademarks are the property of their respective owners.

